Microsoft Privacy Statement

Last Updated: August 2023 What's new?

Personal data we collect

Microsoft collects data from you, through our interactions with you and through our products for a variety of purposes described below, including to operate effectively and provide you with the best experiences with our products. You provide some of this data directly, such as when you create a Microsoft account, administer your organization's licensing account, submit a search query to Bing, register for a Microsoft event, speak a voice command to Cortana, upload a document to OneDrive, sign up for Microsoft 365, or contact us for support. We get some of it by collecting data about your interactions, use, and experience with our products and communications.

We rely on a variety of legal reasons and permissions (sometimes called “legal bases”) to process data, including with your consent, a balancing of legitimate interests, necessity to enter into and perform contracts, and compliance with legal obligations, for a variety of purposes described below.

We also obtain data from third parties. We protect data obtained from third parties according to the practices described in this statement, plus any additional restrictions imposed by the source of the data. These third-party sources vary over time and include:

- Data brokers from which we purchase demographic data to supplement the data we collect.
- Services that make user-generated content from their service available to others, such as local business reviews or public social media posts.
- Communication services, including email providers and social networks, when you give us permission to access your data on such third-party services or networks.

- Service providers that help us determine your device's location.
- Partners with which we offer co-branded services or engage in joint marketing activities.
- Developers who create experiences through or for Microsoft products.
- Third parties that deliver experiences through Microsoft products.
- Publicly-available sources, such as open public sector, academic, and commercial data sets and other data sources.

If you represent an organization, such as a business or school, that utilizes Enterprise and Developer Products from Microsoft, please see the Enterprise and developer products section of this privacy statement to learn how we process your data. If you are an end user of a Microsoft product or a Microsoft account provided by your organization, please see the Products provided by your organization and the Microsoft account sections for more information.

You have choices when it comes to the technology you use and the data you share. When you are asked to provide personal data, you can decline.

Many of our products require some personal data to operate and provide you with a service. If you choose not to provide data required to operate and provide you with a product or feature, you cannot use that product or feature. Likewise, where we need to collect personal data by law or to enter into or carry out a contract with you, and you do not provide the data, we will not be able to enter into the contract; or if this relates to an existing product you're using, we may have to suspend or cancel it. We will notify you if this is the case at the time. Where providing the data is optional, and you choose not to share personal data, features like personalization that use the data will not work for you.

The data we collect depends on the context of your interactions with Microsoft and the choices you make (including your privacy settings), the products and features you use, your location, and applicable law.

The data we collect can include the following:

Name and contact data. Your first and last name, email address, postal address, phone number, and other similar contact data.

Credentials. Passwords, password hints, and similar security information used for authentication and account access.

Demographic data. Data about you such as your age, gender, country, and preferred language.

Payment data. Data to process payments, such as your payment instrument number (such as a credit card number) and the security code associated with your payment instrument.

Subscription and licensing data. Information about your subscriptions, licenses, and other entitlements.

Interactions. Data about your use of Microsoft products. In some cases, such as search queries, this is data you provide in order to make use of the products. In other cases, such as error reports, this is data we generate. Other examples of interactions data include:

- **Device and usage data**. Data about your device and the product and features you use, including information about your hardware and software, how our products perform, as well as your settings. For example:

- **Payment and account history**. Data about the items you purchase and activities associated with your account.
- **Browse history**. Data about the webpages you visit.
- **Device, connectivity, and configuration data**. Data about your device, your device configuration, and nearby networks. For example, data about the operating systems and other software installed on your device, including product keys. In addition, IP address, device identifiers (such as the IMEI number for phones), regional and language settings, and information about WLAN access points near your device.
- **Error reports and performance data**. Data about the performance of the products and any problems you experience, including error reports. Error reports (sometimes called “crash dumps”) can include details of the software or hardware related to an error, contents of files opened when an error occurred, and data about other software on your device.

    - **Troubleshooting and help data**. Data you provide when you contact Microsoft for help, such as the products you use, and other details that help us provide support. For example, contact or authentication data, the content of your chats and other communications with Microsoft, data about the condition of your device, and the products you use related to your help inquiry. When you contact us, such as for customer support, phone conversations or chat sessions with our representatives may be monitored and recorded.
    - **Bot usage data**. Interactions with bots and skills available through Microsoft products, including bots and skills provided by third parties.
- **Interests and favorites**. Data about your interests and favorites, such as the sports teams you follow, the programming languages you prefer, the stocks you track, or cities you add to track things like weather or traffic. In addition to those you explicitly provide, your interests and favorites can also be inferred or derived from other data we collect.

- **Content consumption data**. Information about media content (e.g., TV, video, music, audio, text books, apps, and games) you access through our products.
- **Searches and commands**. Search queries and commands when you use Microsoft products with search or related productivity functionality, such as interactions with a chat bot.
- **Voice data**. Your voice data, sometimes referred to as “voice clips”, such as search queries, commands, or dictation you speak, which may include background sounds.
- **Text, inking, and typing data**. Text, inking, and typing data and related information. For example, when we collect inking data, we collect information about the placement of your inking instrument on your device.
- **Images**. Images and related information, such as picture metadata. For example, we collect the image you provide when you use a Bing image-enabled service.
- **Contacts and relationships**. Data about your contacts and relationships if you use a product to share information with others, manage

contacts, communicate with others, or improve your productivity.

- **Social data**. Information about your relationships and interactions between you, other people, and organizations, such as types of engagement (e.g., likes, dislikes, events, etc.) related to people and organizations.
- **Location data**. Data about your device's location, which can be either precise or imprecise. For example, we collect location data using Global Navigation Satellite System (GNSS) (e.g., GPS) and data about nearby cell towers and Wi-Fi hotspots. Location can also be inferred from a device's IP address or data in your account profile that indicates where it is located with less precision, such as at a city or postal code level.
- **Other input**. Other inputs provided when you use our products. For example, data such as the buttons you press on an Xbox wireless controller using the Xbox network, skeletal tracking data when you use Kinect, and other sensor data, like the number of steps you take, when you use devices that have applicable sensors. And, if you use Spend, at your

direction, we also collect financial transaction data from your credit card issuer to provide the service. If you attend an in-store event, we collect the data you provide to us when registering for or during the event and if you enter into a prize promotion, we collect the data you input into the entry form.

Content. Content of your files and communications you input, upload, receive, create, and control. For example, if you transmit a file using Skype to another Skype user, we need to collect the content of that file to display it to you and the other user. If you receive an email using Outlook.com, we need to collect the content of that email to deliver it to your inbox, display it to you, enable you to reply to it, and store it for you until you choose to delete it. Other content we collect when providing products to you include:

- Communications, including audio, video, text (typed, inked, dictated, or otherwise), in a message, email, call, meeting request, or chat.
- Photos, images, songs, movies, software, and other media or documents you store, retrieve, or otherwise process with our cloud.

Video or recordings. Recordings of events and activities at Microsoft buildings, retail spaces, and other locations. If you enter Microsoft Store locations or other facilities, or attend a Microsoft event that is recorded, we may process your image and voice data.

Feedback and ratings. Information you provide to us and the content of messages you send to us, such as feedback, survey data, and product reviews you write.

Traffic data. Data generated through your use of Microsoft's communications services. Traffic data indicates with whom you have communicated and when your communications occurred. We will process your traffic data only as required to provide, maintain, and improve our communications services and we do so with your consent.

Product-specific sections below describe data collection practices applicable to use of those products.

How we use personal data

Microsoft uses the data we collect to provide you rich, interactive experiences. In particular, we use data to:

- Provide our products, which includes updating, securing, and troubleshooting, as well as providing support. It also includes sharing data, when it is required to provide the service or carry out the transactions you request.
- Improve and develop our products.
- Personalize our products and make recommendations.
- Advertise and market to you, which includes sending promotional communications, targeting advertising, and presenting you relevant offers.

We also use the data to operate our business, which includes analyzing our performance, meeting our legal obligations, developing our workforce, and doing research.

For these purposes, we combine data we collect from different contexts (for example, from your use of two Microsoft products). For example, Cortana may use information from your calendar to suggest action items in a heads-up email, and Microsoft Store uses information about the apps

and services you use to make personalized app recommendations. However, we have built in technological and procedural safeguards designed to prevent certain data combinations where required by law. For example, where required by law, we store data we collect from you when you are unauthenticated (not signed in) separately from any account information that directly identifies you, such as your name, email address, or phone number.

Our processing of personal data for these purposes includes both automated and manual (human) methods of processing. Our automated methods often are related to and supported by our manual methods. For example, to build, train, and improve the accuracy of our automated methods of processing (including artificial intelligence or AI), we manually review some of the predictions and inferences produced by the automated methods against the underlying data from which the predictions and inferences were made. For instance, with your permission and for the purpose of improving our speech recognition technologies, we manually review short snippets of voice data that we have taken steps to de-identify. This

manual review may be conducted by Microsoft employees or vendors who are working on Microsoft's behalf.

When we process personal data about you, we do so with your consent and/or as required to provide the products you use, operate our business, meet our contractual and legal obligations, protect the security of our systems and our customers, or fulfill other legitimate interests of Microsoft as described in this section and in the Reasons we share personal data section of this privacy statement. When we transfer personal data from the European Economic Area, we do so based on a variety of legal mechanisms, as described in the Where we store and process personal data section of this privacy statement.

More on the purposes of processing:

- **Provide our products**. We use data to operate our products and provide you with rich, interactive experiences. For example, if you use OneDrive, we process the documents you upload to OneDrive to enable you to retrieve, delete, edit, forward, or otherwise process it, at your direction as part of the service. Or, for

example, if you enter a search query in the Bing search engine, we use that query to display search results to you. Additionally, as communications are a feature of various products, programs, and activities, we use data to contact you. For example, we may contact you by phone or email or other means to inform you when a subscription is ending or discuss your licensing account. We also communicate with you to secure our products, for example by letting you know when product updates are available.

- **Product improvement**. We use data to continually improve our products, including adding new features or capabilities. For example, we use error reports to improve security features, search queries and clicks in Bing to improve the relevancy of the search results, usage data to determine what new features to prioritize, and voice data to develop and improve speech recognition accuracy.
- **Personalization**. Many products include personalized features, such as recommendations that enhance your productivity and enjoyment. These features use

automated processes to tailor your product experiences based on the data we have about you, such as inferences we make about you and your use of the product, activities, interests, and location. For example, depending on your settings, if you stream movies in a browser on your Windows device, you may see a recommendation for an app from the Microsoft Store that streams more efficiently. If you have a Microsoft account, with your permission, we can sync your settings on several devices. Many of our products provide controls to disable personalized features.

- **Product activation**. We use data—such as device and application type, location, and unique device, application, network, and subscription identifiers—to activate products that require activation.
- **Product development**. We use data to develop new products. For example, we use data, often de-identified, to better understand our customers' computing and productivity needs which can shape the development of new products.

- **Customer support**. We use data to troubleshoot and diagnose product problems, repair customers' devices, and provide other customer care and support services, including to help us provide, improve, and secure the quality of our products, services, and training, and to investigate security incidents. Call recording data may also be used to authenticate or identify you based on your voice to enable Microsoft to provide support services and investigate security incidents.
- **Help secure and troubleshoot**. We use data to help secure and troubleshoot our products. This includes using data to protect the security and safety of our products and customers, detecting malware and malicious activities, troubleshooting performance and compatibility issues to help customers get the most out of their experiences, and notifying customers of updates to our products. This may include using automated systems to detect security and safety issues.
- **Safety**. We use data to protect the safety of our products and our customers. Our security features and products can disrupt the operation

of malicious software and notify users if malicious software is found on their devices. For example, some of our products, such as Outlook.com or OneDrive, systematically scan content in an automated manner to identify suspected spam, viruses, abusive actions, or URLs that have been flagged as fraud, phishing, or malware links; and we reserve the right to block delivery of a communication or remove content if it violates our terms. **In accordance with European Union Regulation (EU) 2021/1232, we have invoked the derogation permitted by that Regulation from Articles 5(1) and 6(1) of EU Directive 2002/58/EC. We use scanning technologies to create digital signatures (known as "hashes") of certain images and video content on our systems. These technologies then compare the hashes they generate with hashes of reported child sexual exploitation and abuse imagery (known as a "hash set"), in a process called "hash matching". Microsoft obtains hash sets from organizations that act in the public interest against child sex abuse. This can result in sharing information with the National Center**

for Missing and Exploited Children (NCMEC) and law enforcement authorities.

- **Updates**. We use data we collect to develop product updates and security patches. For example, we may use information about your device's capabilities, such as available memory, to provide you a software update or security patch. Updates and patches are intended to maximize your experience with our products, help you protect the privacy and security of your data, provide new features, and evaluate whether your device is ready to process such updates.
- **Promotional communications**. We use data we collect to deliver promotional communications. You can sign up for email subscriptions and choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail, and telephone. For information about managing your contact data, email subscriptions, and promotional communications, see the How to access and control your personal data section of this privacy statement.

- **Relevant offers**. Microsoft uses data to provide you with relevant and valuable information regarding our products. We analyze data from a variety of sources to predict the information that will be most interesting and relevant to you and deliver such information to you in a variety of ways. For example, we may predict your interest in gaming and communicate with you about new games you may like.
- **Advertising**. Microsoft does not use what you say in email, human-to-human chat, video calls, or voice mail, or your documents, photos, or other personal files to target ads to you. We use data we collect through our interactions with you, through some of our first-party products, services, apps, and web properties (Microsoft properties), and on third-party web properties, for advertising on our Microsoft properties and on third-party properties. We may use automated processes to help make advertising more relevant to you. For more information about how your data is used for advertising, see the Advertising section of this privacy statement.

- **Prize promotions and events**. We use your data to administer prize promotions and events available in our physical Microsoft Stores. For example, if you enter into a prize promotion, we may use your data to select a winner and provide the prize to you if you win. Or, if you register for a coding workshop or gaming event, we will add your name to the list of expected attendees.
- **Transacting commerce**. We use data to carry out your transactions with us. For example, we process payment information to provide customers with product subscriptions and use contact information to deliver goods purchased from the Microsoft Store.
- **Reporting and business operations**. We use data to analyze our operations and perform business intelligence. This enables us to make informed decisions and report on the performance of our business.
- **Protecting rights and property**. We use data to detect and prevent fraud, resolve disputes, enforce agreements, and protect our property. For example, we use data to confirm the validity of software licenses to reduce piracy. We may

use automated processes to detect and prevent activities that violate our rights and the rights of others, such as fraud.

- **Legal compliance**. We process data to comply with law. For example, we use the age of our customers to assist us in meeting our obligations to protect children's privacy. We also process contact information and credentials to help customers exercise their data protection rights.
- **Research.** With appropriate technical and organizational measures to safeguard individuals' rights and freedoms, we use data to conduct research, including for public interest and scientific purposes.

Reasons we share personal data

We share your personal data with your consent or as necessary to complete any transaction or provide any product you have requested or authorized. For example, we share your content with third parties when you tell us to do so, such as when you send an email to a friend, share photos and documents on OneDrive, or link accounts with another service. If you use a Microsoft product

provided by an organization you are affiliated with, such as an employer or school, or use an email address provided by such organization to access Microsoft products, we share certain data, such as interaction data and diagnostic data to enable your organization to manage the products. When you provide payment data to make a purchase, we will share payment data with banks and other entities that process payment transactions or provide other financial services, and for fraud prevention and credit risk reduction. Additionally, when you save a payment method (such as a card) to your account that you and other Microsoft account holders use to make purchases from Microsoft or its affiliates, your purchase receipts may be shared with anyone else who uses and has access to the same payment method to make a purchase from Microsoft, including the payment method's named accountholder. When you permit push notifications for Microsoft products or applications on a non-Windows device, the operating system of that device will process some personal data to provide push notifications. Accordingly, Microsoft may send data to an external, third-party notification provider to deliver push notifications. Your device's

push notification services are governed by their own service-specific terms and privacy statements.

In addition, we share personal data among Microsoft-controlled affiliates and subsidiaries. We also share personal data with vendors or agents working on our behalf for the purposes described in this statement. For example, companies we've hired to provide customer service support or assist in protecting and securing our systems and services may need access to personal data to provide those functions. In such cases, these companies must abide by our data privacy and security requirements and are not allowed to use personal data they receive from us for any other purpose. We may also disclose personal data as part of a corporate transaction such as a merger or sale of assets.

Finally, we will retain, access, transfer, disclose, and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to do any of the following:

- Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies.
- Protect our customers, for example, to prevent spam or attempts to defraud users of our products, or to help prevent the loss of life or serious injury of anyone.
- Operate and maintain the security of our products, including to prevent or stop an attack on our computer systems or networks.
- Protect the rights or property of Microsoft, including enforcing the terms governing the use of the services—however, if we receive information indicating that someone is using our services to traffic in stolen intellectual or physical property of Microsoft, we will not inspect a customer's private content ourselves, but we may refer the matter to law enforcement.

For more information about data we disclose in response to requests from law enforcement and other government agencies, please see our Law Enforcement Requests Report.

Please note that some of our products include links to or otherwise enable you to access

products of third parties whose privacy practices differ from those of Microsoft. If you provide personal data to any of those products, your data is governed by their privacy policies.

How to access and control your personal data

You can also make choices about the collection and use of your data by Microsoft. You can control your personal data that Microsoft has obtained, and exercise your data protection rights, by contacting Microsoft or using various tools we provide. In some cases, your ability to access or control your personal data will be limited, as required or permitted by applicable law. How you can access or control your personal data will also depend on which products you use. For example, you can:

- Control the use of your data for personalized advertising from Microsoft by visiting our opt-out page.
- Choose whether you wish to receive promotional emails, SMS messages, telephone calls, and postal mail from Microsoft.

- Access and clear some of your data through the Microsoft privacy dashboard.

Not all personal data processed by Microsoft can be accessed or controlled via the tools above. If you want to access or control personal data processed by Microsoft that is not available via the tools above or directly through the Microsoft products you use, you can always contact Microsoft at the address in the How to contact us section or by using our web form.

We provide aggregate metrics about user requests to exercise their data protection rights via the Microsoft Privacy Report.

You can access and control your personal data that Microsoft has obtained with tools Microsoft provides to you, which are described below, or by contacting Microsoft. For instance:

- If Microsoft obtained your consent to use your personal data, you can withdraw that consent at any time.
- You can request access to, erasure of, and updates to your personal data.
- If you'd like to port your data elsewhere, you can use tools Microsoft provides to do so, or if none

are available, you can contact Microsoft for assistance.

You can also object to or restrict the use of your personal data by Microsoft. For example, you can object at any time to our use of your personal data:

- For direct marketing purposes.
- Where we are performing a task in the public interest or pursuing our legitimate interests or those of a third party.

You may have these rights under applicable laws, including the EU General Data Protection Regulation (GDPR), but we offer them regardless of your location. In some cases, your ability to access or control your personal data will be limited, as required or permitted by applicable law.

If your organization, such as your employer, school, or service provider, provides you with access to and is administering your use of Microsoft products, contact your organization to learn more about how to access and control your personal data.

You can access and control your personal data that Microsoft has obtained, and exercise your

data protection rights, using various tools we provide. The tools most useful to you will depend on our interactions with you and your use of our products. Here is a general list of tools we provide to help you control your personal data; specific products may provide additional controls.

- **Bing.** If you are signed into Bing, you can view and clear your stored search and chat history on your privacy dashboard. If you are not signed into Bing, you can view and clear stored search history associated to your device in your Bing settings.
- **Cortana.** You can control some of the data Cortana accesses or stores in your Cortana settings.
- **Microsoft account.** If you wish to access, edit, or remove the profile information and payment information in your Microsoft account, change your password, add security information or close your account, you can do so by visiting the Microsoft account website.
- If you have a **Microsoft Developer Network** (MSDN) public profile, you can access and edit your data by signing in at MSDN forum.

- **Microsoft privacy dashboard**. You can control some of the data Microsoft processes through your use of a Microsoft account on the Microsoft privacy dashboard. From here, for example, you can view and clear the browsing, search, and location data associated with your Microsoft account.
- **Microsoft Store.** You can access your Microsoft Store profile and account information by visiting Microsoft Store and selecting **View account** or **Order history.**
- **Microsoft Teams for personal use.** You can find out how to export or delete Teams data relating to your personal Microsoft account by visiting this page.
- **OneDrive.** You can view, download, and delete your files and photos in OneDrive by signing into your OneDrive.
- **Outlook.com.** You can download your emails in Outlook.com by signing into your account and navigating to your **Privacy and data** settings.
- **Skype**. If you wish to access, edit, or remove some profile and payment information for Skype or change your password, sign in to your account. If you wish to export your Skype chat

history and files shared on Skype, you can request a copy.

- **Volume Licensing Service Center (VLSC).** If you are a Volume Licensing customer, you can control your contact information and subscription and licensing data in one location by visiting the Volume Licensing Service Center website.
- **Xbox**. If you use the Xbox network or Xbox.com, you can view or edit your personal data, including billing and account information, privacy settings, and online safety and data sharing preferences by accessing My Xbox on the Xbox console or on the Xbox.com website.

Not all personal data processed by Microsoft can be accessed or controlled via the tools above. If you want to access or control personal data processed by Microsoft that is not available via the tools above or directly through the Microsoft products you use, you can always contact Microsoft at the address in the How to contact us section or by using our web form. We will respond to requests to control your personal data as required by applicable law.

Your communications preferences

You can choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail, and telephone. If you receive promotional email or SMS messages from us and would like to opt out, you can do so by following the directions in that message. You can also make choices about the receipt of promotional email, telephone calls, and postal mail by signing in with your personal Microsoft account, and viewing your communication permissions where you can update contact information, manage Microsoft-wide contact preferences, opt out of email subscriptions, and choose whether to share your contact information with Microsoft partners. If you do not have a personal Microsoft account, you can manage your Microsoft email contact preferences by using this web form. These choices do not apply to mandatory service communications that are part of certain Microsoft products, programs, activities, or to surveys or other informational communications that have their own unsubscribe method.

Your advertising choices

To opt out of receiving personalized advertising from Microsoft, visit our opt-out page. When you opt out, your preference is stored in a cookie that is specific to the web browser you are using. The opt-out cookie has an expiration date of five years. If you delete the cookies on your device, you need to opt out again.

You can also link your opt-out choice with your personal Microsoft account. It will then apply on any device where you use that account and will continue to apply until someone signs in with a different personal Microsoft account on that device. If you delete the cookies on your device, you will need to sign in again for the settings to apply.

For Microsoft-controlled advertising that appears in apps on Windows, you may use the opt-out linked to your personal Microsoft account, or opt out of interest-based advertising by turning off the advertising ID in Windows settings.

Because the data used for interest-based advertising is also used for other required purposes (including providing our products, analytics, and fraud detection), opting out of

interest-based advertising does not stop that data collection. You will continue to get ads, although they may be less relevant to you.

You can opt out of receiving interest-based advertising from third parties we partner with by visiting their sites (see above).

Browser-based controls

When you use a browser, you can control your personal data using certain features. For example:

- **Cookie controls**. You can control the data stored by cookies and withdraw consent to cookies by using the browser-based cookie controls described in the Cookies section of this privacy statement.
- **Tracking protections**. You can control the data third-party sites can collect about you using Tracking Protection in Internet Explorer (versions 9 and up) and Microsoft Edge. This feature will block third-party content, including cookies, from any site that is listed in a Tracking Protection List you add.
- **Browser controls for "Do Not Track."** Some browsers have incorporated "Do Not Track" (DNT) features that can send a signal to the

websites you visit indicating you do not wish to be tracked. Because there is not yet a common understanding of how to interpret the DNT signal, Microsoft services do not currently respond to browser DNT signals. We continue to work with the online industry to define a common understanding of how to treat DNT signals. In the meantime, you can use the range of other tools we provide to control data collection and use, including the ability to opt out of receiving interest-based advertising from Microsoft as described above.

Cookies and similar technologies

Cookies are small text files placed on your device to store data that can be recalled by a web server in the domain that placed the cookie. This data often consists of a string of numbers and letters that uniquely identifies your computer, but it can contain other information as well. Some cookies are placed by third parties acting on our behalf. We use cookies and similar technologies to store and honor your preferences and settings, enable you to sign-in, provide interest-based advertising, combat fraud, analyze how our products perform, and fulfill

other legitimate purposes described below. Microsoft apps use additional identifiers, such as the advertising ID in Windows, for similar purposes, and many of our websites and applications also contain web beacons or other similar technologies, as described below.

Our use of cookies and similar technologies

Microsoft uses cookies and similar technologies for several purposes, depending on the context or product, including:

- **Storing your preferences and settings**. We use cookies to store your preferences and settings on your device, and to enhance your experiences. For example, depending on your settings, if you enter your city or postal code to get local news or weather information on a Microsoft website, we store that data in a cookie so that you will see the relevant local information when you return to the site. Saving your preferences with cookies, such as your preferred language, prevents you from having to set your preferences repeatedly. If you opt out of interest-based advertising, we store your opt-out preference in a cookie on your device.

Similarly, in scenarios where we obtain your consent to place cookies on your device, we store your choice in a cookie.

- **Sign-in and authentication**. We use cookies to authenticate you. When you sign in to a website using your personal Microsoft account, we store a unique ID number, and the time you signed in, in an encrypted cookie on your device. This cookie allows you to move from page to page within the site without having to sign in again on each page. You can also save your sign-in information so you do not have to sign in each time you return to the site.
- **Security**. We use cookies to process information that helps us secure our products, as well as detect fraud and abuse.
- **Storing information you provide to a website**. We use cookies to remember information you shared. When you provide information to Microsoft, such as when you add products to a shopping cart on Microsoft websites, we store the data in a cookie for the purpose of remembering the information.
- **Social media**. Some of our websites include social media cookies, including those that

enable users who are signed in to the social media service to share content via that service.

- **Feedback**. Microsoft uses cookies to enable you to provide feedback on a website.
- **Interest-based advertising**. Microsoft uses cookies to collect data about your online activity and identify your interests so that we can provide advertising that is most relevant to you. You can opt out of receiving interest-based advertising from Microsoft as described in the How to access and control your personal data section of this privacy statement.
- **Showing advertising**. Microsoft uses cookies to record how many visitors have clicked on an advertisement and to record which advertisements you have seen, for example, so you do not see the same one repeatedly.
- **Analytics**. We use first- and third-party cookies and other identifiers to gather usage and performance data. For example, we use cookies to count the number of unique visitors to a web page or service and to develop other statistics about the operations of our products.
- **Performance**. Microsoft uses cookies to understand and improve how our products

perform. For example, we use cookies to gather data that helps with load balancing; this helps us keep our websites remain up and running.

Where required, we obtain your consent prior to placing or using optional cookies that are not (i) strictly necessary to provide the website; or (ii) for the purpose of facilitating a communication. Please see the “How to Control Cookies” section below for more information.

Some of the cookies we commonly use are listed below. This list is not exhaustive, but it is intended to illustrate the primary purposes for which we typically set cookies. If you visit one of our websites, the site will set some or all of the following cookies:

- **MSCC**. Contains user choices for most Microsoft properties.
- **MUID, MC1, and MSFPC**. Identifies unique web browsers visiting Microsoft sites. These cookies are used for advertising, site analytics, and other operational purposes.
- **ANON**. Contains the ANID, a unique identifier derived from your Microsoft account, which is used for advertising, personalization, and

operational purposes. It is also used to preserve your choice to opt out of interest-based advertising from Microsoft if you have chosen to associate the opt-out with your Microsoft account.

- **CC**. Contains a country code as determined from your IP address.
- **PPAuth, MSPAuth, MSNRPSAuth, KievRPSAuth, WLSSC, MSPProf**. Helps to authenticate you when you sign in with your Microsoft account.
- **MC0**. Detects whether cookies are enabled in the browser.
- **MS0**. Identifies a specific session.
- **NAP**. Contains an encrypted version of your country, postal code, age, gender, language and occupation, if known, based on your Microsoft account profile.
- **MH**. Appears on co-branded sites where Microsoft is partnering with an advertiser. This cookie identifies the advertiser, so the right ad is selected.
- **childinfo, kcdob, kcrelid, kcru, pcfm**. Contains information that Microsoft account uses within its pages in relation to child accounts.

- **MR**. This cookie is used by Microsoft to reset or refresh the MUID cookie.
- **x-ms-gateway-slice**. Identifies a gateway for load balancing.
- **TOptOut**. Records your decision not to receive interest-based advertising delivered by Microsoft. Where required, we place this cookie by default and remove it when you consent to interest-based advertising.

We may also use the cookies of other Microsoft affiliates, companies, and partners, such as LinkedIn and Xandr.

Third Party Cookies

In addition to the cookies Microsoft sets when you visit our websites, we also use cookies from third parties to enhance the services on our sites. Some third parties can also set cookies when you visit Microsoft sites. For example:

- Companies we hire to provide services on our behalf, such as site analytics, place cookies when you visit our sites.
- Companies that deliver content on Microsoft sites, such as videos or news, or ads, place cookies on their own.

These companies use the data they process in accordance with their privacy policies, which may enable these companies to collect and combine information about your activities across websites, apps, or online services.

The following types of third-party cookies may be used, depending on the context, service or product, as well as your settings and permissions:

- **Social Media cookies.** We and third parties use social media cookies to show you ads and content based on your social media profiles and activity on our websites. They're used to connect your activity on our websites to your social media profiles so the ads and content you see on our websites and on social media will better reflect your interests.
- **Analytics cookies.**We allow third parties to use analytics cookies to understand how you use our websites so we can make them better and the third parties can develop and improve their products, which they may use on websites that are not owned or operated by Microsoft. For example, analytics cookies are used to gather information about the pages you visit and how

many clicks you need to accomplish a task. These cookies may also be used for advertising purposes.

- **Advertising cookies.**We and third parties use advertising cookies to show you new ads by recording which ads you've already seen. They're also used to track which ads you click on or purchases you make after clicking on an ad for payment purposes, and to show you ads that are more relevant to you. For example, they're used to detect when you click on an ad and show you ads based on your social media interests and website browsing history.
- **Required cookies.**We use required cookies to perform essential website functions. For example, to log you in, save your language preferences, provide a shopping cart experience, improve performance, route traffic between web servers, detect the size of your screen, determine page load times, and measure audiences. These cookies are necessary for our websites to work.

Where required, we obtain your consent prior to placing or using optional cookies that are not (i)

strictly necessary to provide the website; or (ii) for the purpose of facilitating a communication.

For a list of the third parties that set cookies on our websites, including service providers acting on our behalf, please visit our third party cookie inventory. The third party cookie inventory also includes links to those third parties' websites or privacy notices. Please consult the third party websites or privacy notices for more information on their privacy practices with respect to their cookies that may be set on our websites. On some of our websites, a list of third parties is available directly on the site. The third parties on these sites may not be included in the list on our third party cookie inventory.

How to control cookies

Most web browsers automatically accept cookies but provide controls that allow you to block or delete them. For example, in Microsoft Edge, you can block or delete cookies by selecting **Settings** > **Privacy and services** > **Clear Browsing data** > **Cookies and other site data**. For more information about how to delete your cookies in Microsoft browsers, see Microsoft Edge, Microsoft Edge

Legacy, or Internet Explorer. If you use a different browser, refer to that browser's instructions.

As mentioned above, where required, we obtain your consent before placing or using optional cookies that are not (i) strictly necessary to provide the website; or (ii) for the purpose of facilitating a communication. We separate these optional cookies by purpose, such as for advertising and social media purposes. You may consent to certain categories of optional cookies and not others. You also may adjust your choices by clicking "Manage cookies" in the footer of the website or through the settings made available on the website. Certain features of Microsoft products depend on cookies. If you choose to block cookies, you cannot sign in or use some of those features, and preferences that are dependent on cookies will be lost. If you choose to delete cookies, any settings and preferences controlled by those cookies, including advertising preferences, are deleted and will need to be recreated.

Additional privacy controls that can impact cookies, including the tracking protections feature

of Microsoft browsers, are described in the How to access and control your personal data section of this privacy statement.

Our use of web beacons and analytics services

Some Microsoft webpages contain electronic tags known as web beacons that we use to help deliver cookies on our websites, count users who have visited those websites, and deliver co-branded products. We also include web beacons or similar technologies in our electronic communications to determine whether you open and act on them.

In addition to placing web beacons on our own websites, we sometimes work with other companies to place our web beacons on their websites or in their advertisements. This helps us to, for example, develop statistics on how often clicking on an advertisement on a Microsoft website results in a purchase or other action on the advertiser's website. It also allows us to understand your activity on the website of a Microsoft partner in connection with your use of a Microsoft product or service.

Finally, Microsoft products often contain web beacons or similar technologies from third-party

analytics providers, which help us compile aggregated statistics about the effectiveness of our promotional campaigns or other operations. These technologies enable the analytics providers to set or read their own cookies or other identifiers on your device, through which they can collect information about your online activities across applications, websites, or other products. However, we prohibit these analytics providers from using web beacons on our sites to collect or access information that directly identifies you (such as your name or email address). You can opt out of data collection or use by some of these analytics providers by visiting any of the following sites: Adjust, AppsFlyer, Clicktale, Flurry Analytics, Google Analytics (requires you to install a browser add-on), Kissmetrics, Mixpanel, Nielsen, Acuity Ads, WebTrends, or Optimizely.

Other similar technologies

In addition to standard cookies and web beacons, our products can also use other similar technologies to store and read data files on your computer. This is typically done to maintain your preferences or to improve speed and performance

by storing certain files locally. But, like standard cookies, these technologies can also store a unique identifier for your computer, which can then track behavior. These technologies include Local Shared Objects (or "Flash cookies") and Silverlight Application Storage.

Local Shared Objects or "Flash cookies." Websites that use Adobe Flash technologies can use Local Shared Objects or "Flash cookies" to store data on your computer. To learn how to manage or block Flash cookies, go to the Flash Player help page.

Silverlight Application Storage. Websites or applications that use Microsoft Silverlight technology also have the ability to store data by using Silverlight Application Storage. To learn how to manage or block such storage, see the Silverlight section of this privacy statement.

Products provided by your organization—notice to end users

If you use a Microsoft product with an account provided by an organization you are affiliated with, such as your work or school account, that organization can:

- Control and administer your Microsoft product and product account, including controlling privacy-related settings of the product or product account.
- Access and process your data, including the interaction data, diagnostic data, and the contents of your communications and files associated with your Microsoft product and product accounts.

If you lose access to your work or school account (in event of change of employment, for example), you may lose access to products and the content associated with those products, including those you acquired on your own behalf, if you used your work or school account to sign in to such products.

Many Microsoft products are intended for use by organizations, such as schools and businesses. Please see the Enterprise and developer products section of this privacy statement. If your organization provides you with access to Microsoft products, your use of the Microsoft products is subject to your organization's policies, if any. You should direct your privacy inquiries, including any

requests to exercise your data protection rights, to your organization's administrator. When you use social features in Microsoft products, other users in your network may see some of your activity. To learn more about the social features and other functionality, please review documentation or help content specific to the Microsoft product. Microsoft is not responsible for the privacy or security practices of our customers, which may differ from those set forth in this privacy statement.

When you use a Microsoft product provided by your organization, Microsoft's processing of your personal data in connection with that product is governed by a contract between Microsoft and your organization. Microsoft processes your personal data to provide the product to your organization and you, and in some cases for Microsoft's business operations related to providing the product as described in the Enterprise and developer products section. As mentioned above, if you have questions about Microsoft's processing of your personal data in connection with providing products to your organization, please contact your organization. If

you have questions about Microsoft's business operations in connection with providing products to your organization as provided in the Product Terms, please contact Microsoft as described in the How to contact us section. For more information on our business operations, please see the Enterprise and developer products section.

For Microsoft products provided by your K-12 school, including Microsoft 365 Education, Microsoft will:

- not collect or use student personal data beyond that needed for authorized educational or school purposes;
- not sell or rent student personal data;
- not use or share student personal data for advertising or similar commercial purposes, such as behavioral targeting of advertisements to students;
- not build a personal profile of a student, other than for supporting authorized educational or school purposes or as authorized by the parent, guardian, or student of appropriate age; and
- require that our vendors with whom student personal data is shared to deliver the

educational service, if any, are obligated to implement these same commitments for student personal data.

Microsoft account

With a Microsoft account, you can sign into Microsoft products, as well as those of select Microsoft partners. Personal data associated with your Microsoft account includes credentials, name and contact data, payment data, device and usage data, your contacts, information about your activities, and your interests and favorites. Signing into your Microsoft account enables personalization, consistent experiences across products and devices, permits you to use cloud data storage, allows you to make payments using payment instruments stored in your Microsoft account, and enables other features. There are three types of Microsoft account:

- When you create your own Microsoft account tied to your personal email address, we refer to that account as a **personal Microsoft account**.
- When you or your organization (such as an employer or your school) create your Microsoft account tied to your email address provided by

that organization, we refer to that account as a **work or school account**.
- When you or your service provider (such as a cable or internet service provider) create your Microsoft account tied to your email address with your service provider's domain, we refer to that account as a **third-party account**.

Personal Microsoft accounts. The data associated with your personal Microsoft account, and how that data is used, depends on how you use the account.

- **Creating your Microsoft account**. When you create a personal Microsoft account, you will be asked to provide certain personal data and we will assign a unique ID number to identify your account and associated information. While some products, such as those involving payment, require a real name, you can sign in to and use other Microsoft products without providing your real name. Some data you provide, such as your display name, email address, and phone number, can be used to help others find and connect with you within Microsoft products. For example, people who

know your display name, email address, or phone number can use it to search for you on Skype or Microsoft Teams for personal use and send you an invite to connect with them. Note that if you use a work or school email address to create a personal Microsoft account, your employer or school may gain access to your data. In some cases, you will need to change the email address to a personal email address in order to continue accessing consumer-oriented products (such as the Xbox network).

- **Signing in to Microsoft account**. When you sign in to your Microsoft account, we create a record of your sign-in, which includes the date and time, information about the product you signed in to, your sign-in name, the unique number assigned to your account, a unique identifier assigned to your device, your IP address, and your operating system and browser version.
- **Signing in to Microsoft products**. Signing in to your account enables improved personalization, provides seamless and consistent experiences across products and devices, permits you to access and use cloud data storage, allows you to make payments using payment instruments

stored in your Microsoft account, and enables other enhanced features and settings. For example, when you sign in, Microsoft makes information saved to your account available across Microsoft products so important things are right where you need them. When you sign in to your account, you will stay signed in until you sign out. If you add your Microsoft account to a Windows device (version 8 or higher), Windows will automatically sign you in to products that use Microsoft account when you access those products on that device. When you are signed in, some products will display your name or username and your profile photo (if you have added one to your profile) as part of your use of Microsoft products, including in your communications, social interactions, and public posts. Learn more about your Microsoft account, your data, and your choices.

- **Signing in to third-party products**. If you sign in to a third-party product with your Microsoft account, you will share data with the third party in accordance with the third party's privacy policy. The third party will also receive the version number assigned to your account (a

new version number is assigned each time you change your sign-in data); and information that describes whether your account has been deactivated. If you share your profile data, the third party can display your name or user name and your profile photo (if you have added one to your profile) when you are signed in to that third-party product. If you chose to make payments to third-party merchants using your Microsoft account, Microsoft will pass information stored in your Microsoft account to the third party or its vendors (e.g., payment processors) as necessary to process your payment and fulfill your order (such as name, credit card number, billing and shipping addresses, and relevant contact information). The third party can use or share the data it receives when you sign in or make a purchase according to its own practices and policies. **You should carefully review the privacy statement for each product you sign in to and each merchant you purchase from to determine how it will use the data it collects**.

Work or school accounts. The data associated with a work or school account, and how it will be used, is generally similar to the use and collection

of data associated with a personal Microsoft account.

If your employer or school uses Azure Active Directory (AAD) to manage the account it provides you, you can use your work or school account to sign in to Microsoft products, such as Microsoft 365 and Office 365, and third-party products provided to you by your organization. If required by your organization, you will also be asked to provide a phone number or an alternative email address for additional security verification. And, if allowed by your organization, you may also use your work or school account to sign in to Microsoft or third-party products that you acquire for yourself.

If you sign in to Microsoft products with a work or school account, note:

- The owner of the domain associated with your email address may control and administer your account, and access and process your data, including the contents of your communications and files, including data stored in products provided to you by your organization, and products you acquire by yourself.

- Your use of the products is subject to your organization's policies, if any. You should consider both your organization's policies and whether you are comfortable enabling your organization to access your data before you choose to use your work or school account to sign in to products you acquire for yourself.
- If you lose access to your work or school account (if you change employers, for example), you may lose access to products, including content associated with those products, you acquired on your own behalf if you used your work or school account to sign in to such products.
- Microsoft is not responsible for the privacy or security practices of your organization, which may differ from those of Microsoft.
- If your organization is administering your use of Microsoft products, please direct your privacy inquiries, including any requests to exercise your data subject rights, to your administrator. See also the Notice to end users section of this privacy statement.
- If you are uncertain whether your account is a work or school account, please contact your

organization.

Third-party accounts. The data associated with a third-party Microsoft account, and how it will be used, is generally similar to the use and collection of data associated with a personal Microsoft account. Your service provider has control over your account, including the ability to access or delete your account. **You should carefully review the terms the third party provided you to understand what it can do with your account**.

Collection of data from children

For users under the age of 13 or as specified by law in their jurisdiction, certain Microsoft products and services will either block users under that age or will ask them to obtain consent or authorization from a parent or guardian before they can use it, including when creating an account to access Microsoft services. We will not knowingly ask children under that age to provide more data than is required to provide for the product.

Once parental consent or authorization is granted, the child's account is treated much like any other account. The child can access communication

services, like Outlook and Skype, and can freely communicate and share data with other users of all ages. Learn more about parental consent and Microsoft child accounts.

Parents or guardians can change or revoke the consent choices previously made. As the organizer of a Microsoft family group, the parent or guardian can manage a child's information and settings on their Family Safety page and view and delete a child's data on their privacy dashboard. See below for more information about how to access and delete child data.

Below is additional information about the collection of data from children, including more details as related to Xbox.

Accessing and deleting child data. For Microsoft products and services that require parental consent, a parent can view and delete certain data belonging to their child from the parent's privacy dashboard: browsing history, search history, location activity, media activity, apps and service activity, and product and service performance data. To delete this data, a parent can sign in to their privacy dashboard and manage their child's

activities. Please note that a parent's ability to access and/or delete a child's personal information on their privacy dashboard will vary depending on the laws where you are located.

Additionally, a parent can contact our privacy support team through the privacy support form and, following authentication, request that the data types on the privacy dashboard together with the following data be deleted: software, setup, and inventory; device connectivity and configuration; feedback and ratings; fitness and activity; support content; support interactions; and environmental sensor. We process authenticated deletion requests within 30 days of receipt.

Please note that content like emails, contacts, and chats are accessible through in-product experiences. You can find more information about data you are able to control within Microsoft products by visiting our Privacy Frequently Asked Questions (FAQs).

If your child's account is not a part of your Microsoft family group and you do not have access to your child's activity on your privacy dashboard, then you need to submit a request

related to your child's data through the privacy support form. The privacy team will ask for account verification before fulfilling the request.

To delete all of your child's personal information, you must request deletion of the child's account through the close your account form. This link will prompt you to sign in with your child's account credentials. Check that the page shows the correct Microsoft account, and then follow the instructions to request that your child's account be deleted. Learn more about how to close a Microsoft account.

After you submit the request to close your child's account, we will wait 60 days before permanently deleting the account in case you change your mind or need to access something on the account before it is permanently closed and deleted. During the waiting period, the account is marked for closure and permanent deletion, but it still exists. If you want to reopen your child's Microsoft account, just sign in again within that 60-day period. We will cancel the account closure, and the account will be reinstated.

What is Xbox? Xbox is the gaming and entertainment division of Microsoft. Xbox hosts an online network that consists of software and enables online experiences crossing multiple platforms. This network lets your child find and play games, view content, and connect with friends on Xbox and other gaming and social networks. Children can connect to the Xbox network using Xbox consoles, Windows devices, and mobile devices (Android and iPhone).

Xbox consoles are devices your child can use to find and play games, movies, music, and other digital entertainment. When they sign in to Xbox, in apps, games or on a console, we assign a unique identifier to their device. For instance, when their Xbox console is connected to the internet and they sign in to the console, we identify which console and which version of the console's operating system they are using.

Xbox continues to provide new experiences in client apps that are connected to and backed by services such as Xbox network and cloud gaming. When signed in to an Xbox experience, we collect required data to help keep these experiences

reliable, up to date, secure, and performing as expected.

Data we collect when you create an Xbox profile. You as the parent or guardian are required to consent to the collection of personal data from a child under 13 years old or as otherwise specified by your jurisdiction. With your permission, your child can have an Xbox profile and use the online Xbox network. During the child Xbox profile creation, you will sign in with your own Microsoft account to verify that you are an adult organizer in your Microsoft family group. We collect an alternate email address or phone number to boost account security. If your child needs help accessing their account, they will be able to use one of these alternates to validate they own the Microsoft account.

We collect limited information about children, including name, birthdate, email address, and region. When you sign your child up for an Xbox profile, they get a gamertag (a public nickname) and a unique identifier. When you create your child's Xbox profile you consent to Microsoft collecting, using, and

sharing information based on their privacy and communication settings on the Xbox online network. Your child's privacy and communication settings are defaulted to the most restrictive.

Data we collect. We collect information about your child's use of Xbox services, games, apps, and devices including:

- When they sign in and sign out of Xbox, purchase history, and content they obtain.
- Which games they play and apps they use, their game progress, achievements, play time per game, and other play statistics.
- Performance data about Xbox consoles, Xbox Game Pass and other Xbox apps, the Xbox network, connected accessories, and network connection, including any software or hardware errors.
- Content they add, upload, or share through the Xbox network, including text, pictures, and video they capture in games and apps.
- Social activity, including chat data and interactions with other gamers, and connections they make (friends they add and people who follow them) on the Xbox network.

If your child uses an Xbox console or Xbox app on another device capable of accessing the Xbox network, and that device includes a storage device (hard drive or memory unit), usage data will be stored on the storage device and sent to Microsoft the next time they sign in to Xbox, even if they have been playing offline.

Xbox console diagnostic data. If your child uses an Xbox console, the console will send required data to Microsoft. Required data is the minimum data necessary to help keep Xbox safe, secure, up to date, and performing as expected.

Game captures. Any player in a multiplayer game session can record video (game clips) and capture screenshots of their view of the game play. Other players' game clips and screenshots can capture your child's in-game character and gamertag during that session. If a player captures game clips and screenshots on a PC, the resulting game clips might also capture audio chat if your child's privacy and communication settings on the Xbox online network allow it.

Captioning. During Xbox real-time ("party") chat, players may activate a voice-to-text feature that

lets them view that chat as text. If a player activates this feature, Microsoft uses the resulting text data to provide captioning of chat for players who need it. This data may also be used to provide a safe gaming environment and enforce the Community Standards for Xbox.

Data use. Microsoft uses the data we collect to improve gaming products and experiences—making it safer and more fun over time. Data we collect also enables us to provide your child with personalized, curated experiences. This includes connecting them to games, content, services, and recommendations.

Xbox data viewable by others. When your child is using the Xbox network, their online presence (which can be set to "appear offline" or "blocked"), gamertag, game play statistics, and achievements are visible to other players on the network. Depending on how you set your child's Xbox safety settings, they might share information when playing or communicating with others on the Xbox network.

Safety. In order to help make the Xbox network a safe gaming environment and enforce the

Community Standards for Xbox, we may collect and review voice, text, images, videos and in-game content (such as game clips your child uploads, conversations they have, and things they post in clubs and games).

Anti-cheat and fraud prevention. Providing a fair gameplay environment is important to us. We prohibit cheating, hacking, account stealing, and any other unauthorized or fraudulent activity when your child uses an Xbox online game or any network-connected app on their Xbox console, PC, or mobile device. In order to detect and prevent fraud and cheating, we may use anti-cheat and fraud prevention tools, applications, and other technologies. Such technologies may create digital signatures (known as “hashes”) using certain information collected from their Xbox console, PC, or mobile device, and how they use that device. This can include information about the browser, device, activities, game identifiers, and operating system.

Xbox data shared with game and apps publishers. When your child uses an Xbox online game or any network-connected app on their Xbox console, PC,

or mobile device, the publisher of that game or app has access to data about their usage to help the publisher deliver, support, and improve its product. This data may include: your child's Xbox user identifier, gamertag, limited account info such as country and age range, data about your child's in-game communications, any Xbox enforcement activity, game-play sessions (for example, moves made in-game or types of vehicles used in-game), your child's presence on the Xbox network, the time they spend playing the game or app, rankings, statistics, gamer profiles, avatars, or gamerpics, friends lists, activity feeds for official clubs they belong to, official club memberships, and any content they create or submit in the game or app.

Third-party publishers and developers of games and apps have their own distinct and independent relationship with users and their collection and usage of personal data is subject to their specific privacy policies. You should carefully review their policies to determine how they use your child's data. For example, publishers may choose to disclose or display game data (such as on leaderboards) through their own services. You may

find their policies linked from the game or app detail pages in our stores.

Learn more at Data Sharing with Games and Apps.

To stop sharing game or app data with a publisher, remove its games or app from all devices where they have been installed. Some publisher access to your child's data may be revoked at microsoft.com/consent.

Managing child settings. As the organizer of a Microsoft family group, you can manage a child's information and settings on their Family Safety page, as well as their Xbox profile privacy settings from their Xbox Privacy & online safety page.

You can also use the Xbox Family Settings app to manage your child's experience on the Xbox Network including: spending for Microsoft and Xbox stores, viewing your child's Xbox activity, and setting age ratings and the amount of screen time.

Learn more about managing Xbox profiles at Xbox online safety and privacy settings.
Learn more about Microsoft family groups at Simplify your family's life.

Legacy.

- **Xbox 360**. This Xbox console collects limited required diagnostic data. This data helps keep your child's console functioning as expected.
- **Kinect**. The Kinect sensor is a combination of camera, microphone, and infrared sensor that can enable motions and voice to be used to control game play. For example:
  - If you choose, the camera can be used to sign in to the Xbox network automatically using facial recognition. This data stays on the console, is not shared with anyone, and can be deleted at any time.
  - For game play, Kinect will map distances between the joints on your child's body to create a stick figure representation to enable play.
  - The Kinect microphone can enable voice chat between players during play. The microphone also enables voice commands for control of the console, game, or app, or to enter search terms.
  - The Kinect sensor can also be used for audio and video communications through services such as Skype.

Learn more about Kinect at Xbox Kinect and Privacy.

Other important privacy information

Below you will find additional privacy information, such as how we secure your data, where we process your data, and how long we retain your data. You can find more information on Microsoft and our commitment to protecting your privacy at Microsoft Privacy.

Security of personal data

Microsoft is committed to protecting the security of your personal data. We use a variety of security technologies and procedures to help protect your personal data from unauthorized access, use, or disclosure. For example, we store the personal data you provide on computer systems that have limited access and are in controlled facilities. When we transmit highly confidential data (such as a credit card number or password) over the internet, we protect it through the use of encryption. Microsoft complies with applicable

data protection laws, including applicable security breach notification laws.

Where we store and process personal data

Personal data collected by Microsoft may be stored and processed in your region, in the United States, and in any other country where Microsoft or its affiliates, subsidiaries, or service providers operate facilities. Microsoft maintains major data centers in Australia, Austria, Brazil, Canada, Finland, France, Germany, Hong Kong, India, Ireland, Japan, Korea, Luxembourg, Malaysia, the Netherlands, Singapore, South Africa, the United Kingdom, and the United States. Typically, the primary storage location is in the customer's region or in the United States, often with a backup to a data center in another region. The storage location(s) are chosen in order to operate efficiently, to improve performance, and to create redundancies in order to protect the data in the event of an outage or other problem. We take steps to process the data that we collect under this privacy statement

according to this statement's provisions and the requirements of applicable law.

We transfer personal data from the European Economic Area, the United Kingdom, and Switzerland to other countries, some of which have not yet been determined by the European Commission to have an adequate level of data protection. For example, their laws may not guarantee you the same rights, or there may not be a privacy supervisory authority there that is capable of addressing your complaints. When we engage in such transfers, we use a variety of legal mechanisms, including contracts such as the standard contractual clauses published by the European Commission under Commission Implementing Decision 2021/914, to help protect your rights and enable these protections to travel with your data. To learn more about the European Commission's decisions on the adequacy of the protection of personal data in the countries where Microsoft processes personal data, see this article on the European Commission website.

Microsoft Corporation complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Microsoft Corporation has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Microsoft Corporation has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy statement and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF)

program, and to view our certification, please visit the U.S. Department of Commerce's Data Privacy Framework website. The controlled U.S. subsidiaries of Microsoft Corporation, as identified in our self-certification submission, also adhere to the DPF Principles—for more info, see the list of Microsoft U.S. entities or subsidiaries adhering to the DPF Principles.

If you have a question or complaint related to participation by Microsoft in the DPF Frameworks, we encourage you to contact us via our web form. For any complaints related to the DPF Frameworks that Microsoft cannot resolve directly, we have chosen to cooperate with the relevant EU Data Protection Authority, or a panel established by the European data protection authorities, for resolving disputes with EU individuals, the UK Information Commissioner (for UK individuals), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) for resolving disputes with Swiss individuals. Please contact us if you'd like us to direct you to your data protection authority contacts. As further explained in the DPF Principles, binding

arbitration is available to address residual complaints not resolved by other means. Microsoft is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

Individuals whose personal data is protected by Japan's Act on the Protection of Personal Information should refer to the article on the Japanese Personal Information Protection Commission's website (only published in Japanese) for more information on the commission's review of certain countries' personal data protection systems.

Our retention of personal data

Microsoft retains personal data for as long as necessary to provide the products and fulfill the transactions you have requested, or for other legitimate purposes such as complying with our legal obligations, resolving disputes, and enforcing our agreements. Because these needs can vary for different data types, the context of our interactions with you or your use of products, actual retention periods can vary significantly.

Other criteria used to determine the retention periods include:

- **Do customers provide, create, or maintain the data with the expectation we will retain it until they affirmatively remove it?** Examples include a document you store in OneDrive, or an email message you keep in your Outlook.com inbox. In such cases, we would aim to maintain the data until you actively delete it, such as by moving an email from your Outlook.com inbox to the Deleted Items folder, and then emptying that folder (when your Deleted Items folder is emptied, those emptied items remain in our system for up to 30 days before final deletion). (Note that there may be other reasons why the data has to be deleted sooner, for example if you exceed limits on how much data can be stored in your account.)
- **Is there an automated control, such as in the Microsoft privacy dashboard, that enables the customer to access and delete the personal data at any time?** If there is

not, a shortened data retention time will generally be adopted.

- **Is the personal data of a sensitive type?** If so, a shortened retention time would generally be adopted.
- **Has Microsoft adopted and announced a specific retention period for a certain data type?** For example, for Bing search queries, we de-identify stored queries by removing the entirety of the IP address after 6 months, and cookie IDs and other cross-session identifiers that are used to identify a particular account or device after 18 months.
- **Has the user provided consent for a longer retention period?** If so, we will retain data in accordance with your consent.
- **Is Microsoft subject to a legal, contractual, or similar obligation to retain or delete the data?** Examples can include mandatory data retention laws in the applicable jurisdiction, government orders to preserve data relevant to an investigation, or data retained for the purposes of litigation.

Conversely, if we are required by law to remove unlawful content, we will do so.

U.S. State Data Privacy

If you are a U.S. resident, we process your personal data in accordance with applicable U.S. state data privacy laws, including the California Consumer Privacy Act (CCPA). This section of our privacy statement contains information required by the CCPA and other U.S. state data privacy laws and supplements our privacy statement.

Please note that recent changes to the CCPA and other state data privacy laws are set to take effect in 2023; however, the rules implementing some of these laws have not yet been finalized. We are continuously working to better comply with these laws, and we will update our processes and disclosures as these implementing rules are finalized.

Please also see our U.S. State Data Privacy Laws Notice and our Washington State Consumer Health Data Privacy Policy for additional information about the data we

collect, process, share and disclose, and your rights under applicable U.S. state data privacy laws.

Sale. We do not sell your personal data. So, we do not offer an opt-out to the sale of personal data.

Share. We may "share" your personal data, as defined under California and other applicable U.S. state laws, for personalized advertising purposes. As noted in our Advertising section, we do not deliver personalized advertising to children whose birthdate in their Microsoft account identifies them as under 18 years of age.

In the bulleted list below, we outline the categories of data we share for personalized advertising purposes, the recipients of the personal data, and our purposes of processing. For a description of the data included in each category, please see the Personal data we collect section.

Categories of Personal Data

- Name and contact data

    - Recipients: Third parties that perform online advertising services for Microsoft
    - Purposes of Processing: To deliver personalized advertising based on your interests
- Demographic data
    - Recipients: Third parties that perform online advertising services for Microsoft
    - Purposes of Processing: To deliver personalized advertising based on your interests
- Subscription and licensing data
    - Recipients: Third parties that perform online advertising services for Microsoft
    - Purposes of Processing: To deliver personalized advertising based on your interests
- Interactions
    - Recipients: Third parties that perform online advertising services for Microsoft
    - Purposes of Processing: To deliver personalized advertising based on your interests

Please see the Advertising section for more information about our advertising practices, and our U.S. State Data Privacy Laws Notice for more information on "sharing" for personalized advertising purposes under applicable U.S. state laws.

Rights. You have the right to request that we (i) disclose what personal data we collect, use, disclose, share, and sell, (ii) delete your personal data, (iii) correct your personal data, (iv) restrict the use and disclosure of your sensitive data, and (v) opt-out of "sharing" your personal data with third parties for personalized advertising purposes on third party sites. You may make these requests yourself or through an authorized agent. If you use an authorized agent, we provide your agent with detailed guidance on how to exercise your privacy rights. Please see our U.S. State Data Privacy Laws Notice for additional information on how to exercise these rights. Please also see our Washington State Consumer Health Data Privacy Policy for information on the rights available under Washington law.

If you have a Microsoft account, you can exercise your rights through the Microsoft privacy dashboard, which requires you to log in to your Microsoft account. If you have an additional request or questions after using the dashboard, you may contact Microsoft at the address in the How to contact us section, use our web form, or call our US toll free number +1 (844) 931 2038. If you do not have an account, you may exercise your rights by contacting us as described above. We may ask for additional information, such as your country of residence, email address, and phone number to validate your request before honoring the request.

You may indicate your choice to opt-out of the sharing of your personal data with third parties for personalized advertising on third party sites by visiting our sharing opt-out page. You can also control the personalized advertising you see on Microsoft properties by visiting our opt-out page.

We do not use or disclose your sensitive data for purposes other than those listed below,

without your consent, or as permitted or required under applicable laws. So, we do not offer an ability to limit the use of sensitive data.

You have a right not to receive discriminatory treatment if you exercise your privacy rights. We will not discriminate against you if you exercise your privacy rights.

Personal information processing. In the bulleted list below, we outline the categories of personal data we collect, the sources of the personal data, our purposes of processing, and the categories of third-party recipients with whom we provide the personal data. For a description of the data included in each category, please see the Personal data we collect section. Please see the Our retention of personal data section for information on personal data retention criteria.

Categories of Personal Data

- Name and contact data
  - Sources of personal data: Interactions with users and partners with whom we offer co-branded services

    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide our products; respond to customer questions; help, secure, and troubleshoot; and marketing
    - Recipients: Service providers and user-directed entities
- Credentials
    - Sources of personal data: Interactions with users and organizations that represent users
    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide our products; authentication and account access; and help, secure and troubleshoot
    - Recipients: Service providers and user-directed entities
- Demographic data
    - Sources of personal data: Interactions with users and purchases from data brokers
    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide and

personalize our products; product development; help, secure, and troubleshoot; and marketing
    - Recipients: Service providers and user-directed entities
- Payment data
    - Sources of personal data: Interactions with users and financial institutions
    - Purposes of Processing (Collection and Disclosure to Third Parties): Transact commerce; process transactions; fulfill orders; help, secure, and troubleshoot; and detect and prevent fraud
    - Recipients: Service providers and user-directed entities
- Subscription and licensing data
    - Sources of personal data: Interactions with users and organizations that represent users
    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide, personalize, and activate our products; customer support; help, secure, and troubleshoot; and marketing

    - Recipients: Service providers and user-directed entities
- Interactions
    - Sources of personal data: Interactions with users including data Microsoft generates through those interactions
    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide and personalize our products; product improvement; product development; marketing; and help, secure and troubleshoot
    - Recipients: Service providers and user-directed entities
- Content
    - Sources of personal data: Interactions with users and organizations that represent users
    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide our products; safety; and help, secure, and troubleshoot
    - Recipients: Service providers and user-directed entities

- Video or recordings
  - Sources of personal data: Interactions with users and publicly available sources
  - Purposes of Processing (Collection and Disclosure to Third Parties): Provide our products; product improvement; product development; marketing; help, secure, and troubleshoot; and safety
  - Recipients: Service providers and user-directed entities
- Feedback and ratings
  - Sources of personal data: Interactions with users
  - Purposes of Processing (Collection and Disclosure to Third Parties): Provide our products; product improvement; product development; customer support; and help, secure, and troubleshoot
  - Recipients: Service providers and user-directed entities

While the bulleted list above contains the primary sources and purposes of processing for each category of personal data, we also collect personal data from the sources listed

in the Personal data we collect section, such as developers who create experiences through or for Microsoft products. Similarly, we process all categories of personal data for the purposes described in the How we use personal data section, such as meeting our legal obligations, developing our workforce, and doing research.

Subject to your privacy settings, your consent, and depending on the products you use and your choices, we may collect, process, or disclose certain personal data that qualifies as "sensitive data" under applicable U.S. state data privacy laws. Sensitive data is a subset of personal data. In the list below, we outline the categories of sensitive data we collect, the sources of the sensitive data, our purposes of processing, and the categories of third party recipients with whom we share the sensitive data. Please see the Personal data we collect section for more information about the sensitive data we may collect.

Categories of Sensitive Data

- Account log-in, financial account, debit or credit card number, and the means to access the account (security or access code, password, credentials, etc.)
  - Sources of sensitive data: Interactions with users and organizations that represent users
  - Purposes of Processing (Collection and Disclosure to Third Parties): Provide the product and fulfill requested financial transactions
  - Recipients: Service providers and payment processing providers
- Precise geo-location information
  - Sources of sensitive data: Users' interactions with the products
  - Purposes of Processing (Collection and Disclosure to Third Parties): Provide the service requested; product improvement; some attributes may be disclosed to third parties to provide the service
  - Recipients: Users and service providers (please see the Windows Location Services and Recording section of our privacy statement for more information)

- Racial or ethnic origin, religious or philosophical beliefs, or union membership
  - Sources of sensitive data: Communications with users
  - Purposes of Processing (Collection and Disclosure to Third Parties): Conduct research studies to better understand how our products are used and perceived and for the purposes of improving the product experiences
  - Recipients: Service providers
- Medical or mental health, sex life, or sexual orientation
  - Sources of sensitive data: Communications with users
  - Purposes of Processing (Collection and Disclosure to Third Parties): Conduct research studies to better understand how our products are used and perceived and for the purposes of improving the product experiences and accessibility
  - Recipients: Service providers
- Contents of your mail, email, or text messages (where Microsoft is not the

intended recipient of the communication)
    - Sources of sensitive data: Users' interactions with the products
    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide our products; improve the product experience; safety; and help, secure, and troubleshoot
    - Recipients: Service providers
- Personal data collected from a known child under 13 years of age
    - Sources of sensitive data: Interactions with users and organizations that represent users
    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide our products; product improvement; product development; recommendations; help, secure, and troubleshoot; and safety
    - Recipients: Service providers and user-directed entities (in accordance with your Microsoft Family Safety settings)

While the bulleted list above contains the primary sources and purposes of processing

for personal data collected from children under 13, we also collect personal data from the sources listed in the Collection of Data from Children section.

We do not use or disclose your sensitive data for purposes other than the following:

- Perform the services or provide the goods you reasonably expect
- Help ensure the security and integrity of our services, systems, and data, to combat malicious deceptive, fraudulent or illegal acts, and to protect the physical safety of individuals, to the extent the processing is reasonably necessary and proportionate
- For short-term transient use (including non-personalized advertising), so long as the personal data is not disclosed to a third party, is not used for profiling, and is not used to alter an individual's experience outside the current interaction with Microsoft
- Perform services on behalf of Microsoft, such as maintaining accounts, providing customer service, processing, or fulfilling

orders/transactions, verifying customer information, processing payments, providing financing, providing analytics, providing storage, and similar services
- Undertake activities to verify or maintain the quality or safety of, or improve, upgrade, or enhance a service or device owned or controlled by Microsoft
- Collect or process sensitive data where the collection or processing is not for inferring characteristics about the individual
- Any other activities in accordance with any future regulations that are issued pursuant to U.S. state data privacy laws

De-Identified Data. In some situations, Microsoft may process de-identified data. Data is in this state when we are not able to link data to an individual to whom such data may relate without taking additional steps. In those instances, and unless allowed under applicable law, we will maintain such information in a de-identified state, and will not try to re-identify the individual to whom the de-identified data relates.

Disclosures of personal data for business or commercial purposes. As indicated in the Reasons we share personal data section, we share personal data with third parties for various business and commercial purposes. The primary business and commercial purposes for which we share personal data are the purposes of processing listed in the table above. However, we share all categories of personal data for the business and commercial purposes in the Reasons we share personal data section.

Parties that control collection of personal data. In certain situations, we may allow a third party to control the collection of your personal data. For example, third party applications or extensions that run on Windows or Edge browser may collect personal data based on their own practices.

Microsoft allows advertising companies to collect information about your interactions with our websites in order to deliver personalized ads on Microsoft's behalf. These

companies include: Meta, LinkedIn, Google, and Adobe.

Artificial Intelligence

Microsoft leverages the power of artificial intelligence (AI) in many of our products and services, including by incorporating generative AI features. Microsoft's development and use of AI is subject to Microsoft's AI Principles and Microsoft's Responsible AI Standard, and the collection and use of personal data in developing and deploying AI features is consistent with the commitments outlined in this privacy statement. Product-specific details provide additional relevant information. You can find out more about how Microsoft uses AI here.

Advertising

Advertising allows us to provide, support, and improve some of our products. Microsoft does not use what you say in email, human-to-human chat, video calls or voice mail, or your documents, photos, or other personal files to target ads to you. We use other data, detailed

below, for advertising on our Microsoft properties and on third-party properties. For example:

- Microsoft may use data we collect to select and deliver some of the ads you see on Microsoft web properties, such as Microsoft.com, Microsoft Start, and Bing.
- When the advertising ID is enabled in Windows as part of your privacy settings, third parties can access and use the advertising ID (much the same way that websites can access and use a unique identifier stored in a cookie) to select and deliver ads in such apps.
- We may share data we collect with internal and external partners, such as Xandr, Yahoo, or Facebook (see below), so that the ads you see in our products and their products are more relevant and valuable to you.
- Advertisers may choose to place our web beacons on their sites, or use similar technologies, in order to allow Microsoft to collect information on their sites such as activities, purchases, and visits; we use this

data on behalf of our advertising customers to provide ads.

The ads that you see may be selected based on data we process about you, such as your interests and favorites, your location, your transactions, how you use our products, your search queries, or the content you view. For example, if you view content on Microsoft Start about automobiles, we may show advertisements about cars; if you search “pizza places in Seattle” on Bing, you may see advertisements in your search results for restaurants in Seattle.

The ads that you see may also be selected based on other information learned about you over time using demographic data, location data, search queries, interests and favorites, usage data from our products and sites, and the information we collect about you from the sites and apps of our advertisers and partners. We refer to these ads as "personalized advertising" in this statement. For example, if you view gaming content on xbox.com, you may see offers for games on Microsoft Start.

To provide personalized advertising, we combine cookies placed on your device using information that we collect (such as IP address) when your browser interacts with our websites. If you opt out of receiving personalized advertising, data associated with these cookies will not be used.

We may use information about you to serve you with personalized advertising when you use Microsoft services. If you are logged in with your Microsoft account and have consented to allow Microsoft Edge to use your online activity for personalized advertising, you will see offers for products and services based on your online activity while using Microsoft Edge. To configure your privacy settings for Edge, go to Microsoft Edge > Settings > Privacy and Services. To configure your privacy and ad settings for your Microsoft account with respect to your online activity across browsers, including Microsoft Edge, or when visiting third-party websites or apps, go to your dashboard at privacy.microsoft.com.

Further details regarding our advertising-related uses of data include:

- **Advertising industry best practices and commitments**. Microsoft is a member of the Network Advertising Initiative (NAI) and adheres to the NAI Code of Conduct. We also adhere to the following self-regulatory programs:
  - In the US: Digital Advertising Alliance (DAA)
  - In Europe: European Interactive Digital Advertising Alliance (EDAA)
  - In Canada: Ad Choices: Digital Advertising Alliance of Canada (DAAC) / Choix de Pub: l'Alliance de la publicité numérique du Canada (DAAC)
- **Health-related ad targeting**. In the United States, we provide personalized advertising based on a limited number of standard, non-sensitive health-related interest categories, including allergies, arthritis, cholesterol, cold and flu, diabetes, gastrointestinal health, headache / migraine, healthy eating, healthy heart, men's health, oral health, osteoporosis, skin health, sleep, and vision /

eye care. We will also personalize ads based on custom, non-sensitive health-related interest categories as requested by advertisers.

- **Children and advertising**. We do not deliver personalized advertising to children whose birthdate in their Microsoft account identifies them as under 18 years of age.
- **Data retention**. For personalized advertising, we retain data for no more than 13 months, unless we obtain your consent to retain the data longer.
- **Sensitive Data**. Microsoft Advertising does not collect, process, or disclose personal data that qualifies as “sensitive data” under applicable U.S. state data privacy laws for the purposes of providing personalized advertising.
- **Data sharing**. In some cases, we share with advertisers reports about the data we have collected on their sites or ads.

Data collected by other advertising companies. Advertisers sometimes include their own web beacons (or those of their other advertising partners) within their

advertisements that we display, enabling them to set and read their own cookie. Additionally, Microsoft partners with Xandr, a Microsoft company, and third-party ad companies to help provide some of our advertising services, and we also allow other third-party ad companies to display advertisements on our sites. These third parties may place cookies on your computer and collect data about your online activities across websites or online services. These companies currently include, but are not limited to: Facebook, Media.net, Outbrain, Taboola and Yahoo. Select any of the preceding links to find more information on each company's practices, including the choices it offers. Many of these companies are also members of the NAI or DAA, which each provide a simple way to opt out of ad targeting from participating companies.

To opt out of receiving personalized advertising from Microsoft, visit our opt-out page. When you opt out, your preference is stored in a cookie that is specific to the web browser you are using. The opt-out cookie has an expiration date of five years. If you delete

the cookies on your device, you need to opt out again.

Speech recognition technologies

Speech recognition technologies are integrated into many Microsoft products and services. Microsoft provides both device-based speech recognition features and cloud-based (online) speech recognition features. Microsoft's speech recognition technology transcribes voice data into text. With your permission, Microsoft employees and vendors working on behalf of Microsoft, will be able to review snippets of your voice data or voice clips in order to build and improve our speech recognition technologies. These improvements allow us to build better voice-enabled capabilities that benefit users across all our consumer and enterprise products and services. Prior to employee or vendor review of voice data, we protect users' privacy by taking steps to de-identify the data, requiring non-disclosure agreements with relevant vendors and their employees, and requiring that employees and vendors meet high privacy

standards. Learn more about Microsoft and your voice data.

Preview or free-of-charge releases

Microsoft offers preview, insider, beta or other free-of-charge products and features ("previews") to enable you to evaluate them while providing Microsoft with data about your use of the product, including feedback and device and usage data. As a result, previews can automatically collect additional data, provide fewer controls, and otherwise employ different privacy and security measures than those typically present in our products. If you participate in previews, we may contact you about your feedback or your interest in continuing to use the product after general release.

Changes to this privacy statement

We update this privacy statement when necessary to provide greater transparency or in response to:

- Feedback from customer, regulators, industry, or other stakeholders.
- Changes in our products.
- Changes in our data processing activities or policies.

When we post changes to this statement, we will revise the "last updated" date at the top of the statement and describe the changes on the Change history page. If there are material changes to the statement, such as a change to the purposes of processing of personal data that is not consistent with the purpose for which it was originally collected, we will notify you either by prominently posting a notice of such changes before they take effect or by directly sending you a notification. We encourage you to periodically review this privacy statement to learn how Microsoft is protecting your information.

How to contact us

If you have a privacy concern, complaint, or question for the Microsoft Chief Privacy Officer or the Data Protection Officer for your region, please contact us by using our web form. We

will respond to questions or concerns as required by law and within a period no longer than 30 days. You can also raise a concern or lodge a complaint with a data protection authority or other official with jurisdiction.

When Microsoft is a controller, unless otherwise stated, Microsoft Corporation and, for those in the European Economic Area, the United Kingdom, and Switzerland, Microsoft Ireland Operations Limited are the data controllers for personal data we collect through the products subject to this statement. Our addresses are:

- Microsoft Privacy, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, USA. Telephone: +1 (425) 882 8080.
- Microsoft Ireland Operations Limited, Attn: Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland. Telephone: +353 1 706 3117.

To find the Microsoft subsidiary in your country or region, see the list of Microsoft office locations around the world.

If you would like to exercise your rights under applicable U.S. state data privacy law, you may contact Microsoft at the address above, use our web form, or call our U.S. toll free number +1 (844) 931 2038.

If you are a resident of Canada and its provinces you may contact the Microsoft Data Protection Officer for Canada at Microsoft, 1950 Meadowvale Blvd, Mississauga, Ontario, L5N 8L9, at +1 (416) 349 2506, or by using our web form.

Where French law applies, you can also send us specific instructions regarding the use of your personal data after your death, by using our web form.

If you have a technical or support question, please visit Microsoft Support to learn more about Microsoft Support offerings. If you have a personal Microsoft account password question, please visit Microsoft account support.

We offer various means for you to control your personal data that Microsoft has obtained, and to exercise your data protection rights. You

can do so by contacting Microsoft at our web form or the information above, or by using the various tools we provide. Please see the How to access and control your personal data section for additional details.

Enterprise and developer products

Enterprise and Developer Products are Microsoft products and related software offered to and designed primarily for use by organizations and developers. They include:

- Cloud services, referred to as Online Services in the Product Terms, such as Microsoft 365 and Office 365, Microsoft Azure, Microsoft Dynamics365, and Microsoft Intune for which an organization (our customer) contracts with Microsoft for the services ("Enterprise Online Services").
- Other enterprise and developer tools and cloud-based services, such as Azure PlayFab Services (to learn more see Azure PlayFab Terms of Service).
- Server, developer, and hybrid cloud platform products, such as Windows Server, SQL Server, Visual Studio, System Center, Azure Stack and

open source software like Bot Framework solutions (“Enterprise and Developer Software”).
- Appliances and hardware used for storage infrastructure, such as StorSimple (“Enterprise Appliances”).
- Professional services referred to in the Product Terms that are available with Enterprise Online Services, such as onboarding services, data migration services, data science services, or services to supplement existing features in the Enterprise Online Services.

In the event of a conflict between this Microsoft privacy statement and the terms of any agreement(s) between a customer and Microsoft for Enterprise and Developer Products, the terms of those agreement(s) will control.

You can also learn more about our Enterprise and Developer Products’ features and settings, including choices that impact your privacy or your end users’ privacy, in product documentation.

If any of the terms below are not defined in this Privacy Statement or the Product Terms, they have the definitions below.

General. When a customer tries, purchases, uses, or subscribes to Enterprise and Developer Products, or obtains support for or professional services with such products, Microsoft receives data from you and collects and generates data to provide the service (including improving, securing, and updating the service), conduct our business operations, and communicate with the customer. For example:

- When a customer engages with a Microsoft sales representative, we collect the customer's name and contact data, along with information about the customer's organization, to support that engagement.
- When a customer interacts with a Microsoft support professional, we collect device and usage data or error reports to diagnose and resolve problems.
- When a customer pays for products, we collect contact and payment data to process the payment.
- When Microsoft sends communications to a customer, we use data to personalize the content of the communication.

- When a customer engages with Microsoft for professional services, we collect the name and contact data of the customer's designated point of contact and use information provided by the customer to perform the services that the customer has requested.

The Enterprise and Developer Products enable you to purchase, subscribe to, or use other products and online services from Microsoft or third parties with different privacy practices, and those other products and online services are governed by their respective privacy statements and policies.

Enterprise online services

To provide the Enterprise Online Services, Microsoft uses data you provide (including Customer Data, Personal Data, Administrator Data, Payment Data, and Support Data) and data Microsoft collects or generates associated with your use of the Enterprise Online Services. We process data as described in the Product Terms, Microsoft Products and Services Data Protection Addendum (Products and Services DPA), and the Microsoft Trust Center.

Personal Data. Customer is the controller of Personal Data and Microsoft is the processor of such data, except when (a) Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor or (b) as stated otherwise in the standard Products and Services DPA. In addition, as provided in the standard Products and Services DPA, Microsoft has taken on the added responsibilities of a data controller under GDPR when processing Personal Data in connection with its business operations incident to providing its services to Microsoft's commercial customers, such as billing and account management; compensation; internal reporting and business modeling; and financial reporting. We use Personal Data in the least identifiable form that will support processing necessary for these business operations. We rely on statistical data and aggregate pseudonymized Personal Data before using it for our business operations, removing the ability to identify specific individuals.

Administrator Data. Administrator Data is the information provided to Microsoft during sign-

up, purchase, or administration of Enterprise Online Services. We use Administrator Data to provide the Enterprise Online Services, complete transactions, service the account, detect and prevent fraud, and comply with our legal obligations. Administrator Data includes the name, address, phone number, and email address you provide, as well as aggregated usage data related to your account, such as the controls you select. Administrator Data also includes contact information of your colleagues and friends if you agree to provide it to Microsoft for the limited purpose of sending them an invitation to use the Enterprise Online Services; we contact those individuals with communications that include information about you, such as your name and profile photo.

As needed, we use Administrator Data to contact you to provide information about your account, subscriptions, billing, and updates to the Enterprise Online Services, including information about new features, security, or other technical issues. We also contact you regarding third-party inquiries we receive

regarding use of the Enterprise Online Services, as described in your agreement. You cannot unsubscribe from these non-promotional communications. We may also contact you regarding information and offers about other products and services, or share your contact information with Microsoft's partners. When such a partner has specific services or solutions to meet your needs, or to optimize your use of the Enterprise Online Services, we may share limited, aggregated information about your organization’s account with the partner. Microsoft will not share your confidential information or contact information with the authorized partner unless we have sufficient rights to do so. You can manage your contact preferences or update your information in your account profile.

Payment Data. We use payment data to complete transactions, as well as to detect and prevent fraud.

Support Data. Customers provide or authorize Microsoft to collect data in connection with obtaining technical support for the Enterprise

Online Services. We process Support Data to provide technical support and as described in the Products and Services DPA.

Local Software and Diagnostic Data. Some Online Services may require, or may be enhanced by, the installation of local software (e.g., agents, device management applications). The local software may collect Diagnostic Data (as defined in the Products and Services DPA) about the use and performance of that software. That data may be transmitted to Microsoft and used for the purposes described in the Products and Services DPA.

Bing Search Services Data. Bing Search Services, as defined in the Product Terms, use data such as search queries as described in the Bing section of this privacy statement.

Enterprise and developer software and enterprise appliances

Enterprise and developer software and enterprise appliances collect data to operate effectively and provide you the best

experiences. The data we collect depends on the features you use, as well as your configuration and settings, but it is generally limited to device and usage data. Customers have choices about the data they provide. Here are examples of the data we collect:

- During installation or when you upgrade an enterprise and developer software, we may collect device and usage data to learn whether you experience any difficulties.
- When you use enterprise software or enterprise appliances, we may collect device and usage data to learn about your operating environment to improve security features.
- When you experience a crash using enterprise software or enterprise appliances, you may choose to send Microsoft an error report to help us diagnose the problem and deliver customer support.

Microsoft uses the data we collect from enterprise and developer software and enterprise appliances to provide and improve

our products, to deliver customer support, to activate the product, to communicate with you, and to operate our business.

Microsoft SQL Server is a relational database management platform and includes products that can be installed separately (such as SQL Server Management Studio). For detailed information about what data we collect, how we use it, and how to manage your privacy options, visit the SQL Server privacy page. If you work in an organization, your administrator can set certain telemetry settings in SQL Server via Group Policy.

HoloLens. HoloLens headsets are self-contained Windows computers with Wi-Fi connectivity that enable a mixed reality experience for apps and solutions. Microsoft collects diagnostic data to solve problems and to keep Windows running on HoloLens up to date, secure, and operating properly. Diagnostic data also helps us improve HoloLens and related Microsoft products and services depending on the diagnostic data

settings you've chosen for your device. Learn more about Windows diagnostic data.

HoloLens also processes and collects data related to the HoloLens experience and device, which include cameras, microphones, and infrared sensors that enable motions and voice to navigate.

- If you choose, cameras can be used to sign you in automatically using your iris. To do this, HoloLens takes an image of your iris and measures distances between key points to create and store a numeric value that represents only you. This data stays on the HoloLens and is not shared with anyone, and you can choose to delete this data from your HoloLens at any time.
- HoloLens also detects hand gestures intended for system interactions (such as menu navigation, pan/zoom, and scroll). This data is processed on your HoloLens device and is not stored.
- HoloLens derives tracking points based on your environment which allows it to understand surfaces in space and allows

you to place digital assets on them. There are no images associated with this environmental data and it is stored locally on the HoloLens device. You can choose to delete this data from your HoloLens at any time.

The headset's microphones enable voice commands for navigation, controlling apps, or to enter search terms. Learn more about voice data collection.

Productivity and communications products

Productivity and communications products are applications, software, and services you can use to create, store, and share documents, as well as communicate with others.

Microsoft 365 and Office

Microsoft 365, previous versions called Office 365, is a collection of subscription productivity services and applications including Word, Excel, PowerPoint, and Outlook, among others. Office is the one-time purchase version of these applications available on PC or Mac.

Both Microsoft 365 and Office are comprised of client software applications and connected online services (or web apps in the case of Microsoft 365 for the web) that span many platforms and have numerous interdependent experiences. For more details about Outlook, see the Outlook section of this privacy statement.

Various cloud-based Microsoft 365 services enable you to use your file content for designs and recommendations, collaborate with others within your documents, and provide you functionality from other Microsoft products, such as Bing and Cortana, and third-party connected products. If you work in an organization, your administrator may turn off or disable these connected services. You can access the privacy controls within your Microsoft 365 and Office apps. For more information, see Account Privacy Settings.

Office Roaming Service. The Office Roaming Service helps keep your settings, including your privacy settings, up to date across your devices running Microsoft 365 or Office apps.

When you sign in to your apps with either your Microsoft account or an account issued by your organization, the service syncs some of your customized settings to Microsoft servers. For example, the service syncs a list of most recently used documents or the last location viewed within a document. When you sign in to another device with the same account, the Office Roaming Service downloads your settings from Microsoft servers and applies them to the additional device. When you sign out of your apps, the service removes your settings from your device. Any changes you make to your customized settings are sent to Microsoft servers.

Updates from Microsoft. Microsoft uses services such as Click-to-Run, Microsoft AutoUpdate (for Mac), or Microsoft Update (for some versions of Office) to provide you with security and other important updates.

These services can automatically detect the availability of online updates for Microsoft 365 or Office apps on your device and download and install them automatically.

Diagnostic Data. Diagnostic data is used to (i) keep your Microsoft 365 or Office apps secure and up to date; (ii) detect, diagnose, and remediate problems; and (iii) make product improvements. This data does not include a user's name or email address, the content of the user's files, or information about apps unrelated to Microsoft 365 or Office. Users have a choice between two different levels of diagnostic data collection, Required and Optional.

- **Required**. The minimum data necessary to help keep apps secure, up to date, and performing as expected on the device it's installed on.
- **Optional**. Additional data that helps us make product improvements and provides enhanced information to help us detect, diagnose, and remediate issues.

See Diagnostic Data for more information.

Connected Experiences. Microsoft 365 continues to provide more experiences in client applications that are connected to and backed by cloud-based services. A subset of

these connected experiences is also available in Office. If you choose to use connected experiences, required service data will be collected to help keep these connected experiences reliable, up to date, secure, and performing as expected. See below for additional information about required service data.

Working with others on a document stored on OneDrive or translating the contents of a Word document into a different language are examples of connected experiences. There are two types of connected experiences.

- **Experiences that analyze your content**. Experiences that use your file content to provide you with design recommendations, editing suggestions, data insights, and similar features. For example, PowerPoint Designer or Editor in Word.
- **Experiences that download online content**. Experiences that allow you to search and download online content including templates, images, 3D models, videos, and reference materials to enhance your

documents. For example, templates or PowerPoint QuickStarter.

You can access the privacy controls within your Microsoft 365 and Office client apps. These privacy settings allow you to configure your connected experiences. For example, you can choose to enable connected experiences that download online content, but not connected experiences that analyze content. Turning off connected experiences will also turn off additional experiences, such as document co-authoring and online file storage. But even if you use this privacy setting to turn off connected experiences, certain functionality will remain available, such as syncing your mailbox in Outlook, as well as essential services described below. These controls are not available when using Microsoft 365 for the web, since you will already be cloud-connected. For more information about accessing these controls, see Account Privacy Settings.

If you choose to disable certain types of connected experiences, either the ribbon or

menu command for those connected experiences will be grayed out or you will get an error message when you try to use those connected experiences.

Essential services. There are a set of services that are essential to how Microsoft 365 and Office functions and cannot be disabled. For example, the licensing service that confirms that you are properly licensed to use Microsoft 365 is essential. Required service data about these services is collected and sent to Microsoft, regardless of any other settings that you have configured. See Essential Services for more information.

Required service data for connected experiences. As you use a connected experience, data is sent to and processed by Microsoft to provide you that connected experience. This data is necessary because this information enables us to deliver these cloud-based connected experiences. We refer to this data as required service data.

Required service data can include information related to the operation of the connected

experience that is needed to keep the underlying service secure, up to date, and performing as expected. If you choose to use a connected experience that analyzes your content, for example Translate in Word, the text you typed and selected to translate is also sent and processed to provide you the connected experience. Your text and the translation are not stored by our service. Required service data can also include information needed by a connected experience to perform its task, such as configuration information about the Microsoft 365 or Office app.

See Required service data for more information.

Microsoft Family

This section applies to the Microsoft Family Safety M365 product, which allows a family group to connect through the Microsoft Family Safety app on their Windows, Xbox, or mobile devices. Please carefully review the information at Microsoft Family Safety if choosing to create or join a family group.

Microsoft Family Safety can help parents and guardians to create a safer environment for their family group with digital content filtering, screen time limits, spending for Microsoft and Xbox stores, setting age ratings for apps and games, and location sharing. To learn about how Microsoft collects and uses children's data, see the Collection of data from children section of the Privacy Statement. If you are using Microsoft Family Safety in Windows, see the Windows security and safety features section of the Privacy Statement for additional information.

When you have enabled family activity reporting for a child, Microsoft will collect details about how the child uses their devices, such as search, web, app, and game activity, and provide parents with reports of that child's online activities. Activity reports are routinely deleted from Microsoft servers.

Certain Family Safety features, such as Location Sharing, Drive Safety, Share Drives, Places, and Location Alerts will use your location information when enabled. When you

have enabled Location Sharing, for instance, your device will upload location data to the cloud and share it with others in your family group. Microsoft retains only your last known location as part of the Location Sharing feature (each new location replaces the previous one). When you enable Drive Safety, your location will be used to record your drive habits such as whether you are driving within the speed limits, if you're using your phone while driving, and if you accelerate or brake suddenly. These reports will be uploaded to the cloud, and you can choose to share your drive reports with your family group. You can turn off these location features at any time in the Family Safety settings. You can manage your device's location data at the Microsoft Privacy Dashboard. Learn more about Family Safety and your location data.

Microsoft Teams

This section applies to the consumer offering of Teams; if you are using Teams with a school or work account, see the Enterprise and developer products of this privacy statement.

Teams is an all-in-one collaboration and communication hub. Teams lets you stay organised and connected across your entire life. Teams allows you to call people with voice or video calling. Teams allows you to easily find people, files, photos, conversations, tasks, and calendars in one convenient and secure place. Teams allows you to store confidential information like passwords, rewards numbers, or login information and share it with others within Teams. With your consent, you can share your location with friends and family.

As part of providing these features, Microsoft collects data about the usage of the features as well as information about your communications, including the time and date of the communication and users that are part of the communication.

Teams profile. Your Teams profile includes information you provided when you set up a Microsoft account. To enable other people to find you on Teams (or products that interact with Teams for personal use, including Teams for enterprise) your display name and picture

are visible to other users on Teams that have your contact information.

Teams contacts. With your permission, Teams will sync your device, Outlook, and Skype contacts periodically and check for other Teams users that match contacts in your device, Outlook, or Skype address books. You are always in control of your contacts and can stop syncing at any time. If you choose to stop syncing your device, Outlook, or Skype contacts, or you are inactive on your device, any contacts that have not been matched during the synchronization process will be deleted from Teams. If you wish to invite any of your device, Outlook, or Skype contacts to join a conversation, you can invite users to a 1:1 directly, or Microsoft can send an invitation on your behalf via SMS or email for invitations to group conversations. You can block users if you do not want to receive their communications; additionally, you can report a concern to Microsoft.

Notice to non-user contacts. If your information appears in the device, Outlook, or

Skype address books of a Teams user who chooses to sync their device, Outlook, or Skype contacts with their Teams contacts, Microsoft may process your data in order to determine whether you are a current Teams user and to allow Teams users to invite you to the service, including via SMS and email. As long as the Teams user continues to be active on Teams on their device and continues to enable contact syncing with the applicable device or service, your information will be stored on our servers and we will periodically process your information as a part of the Teams user's contact syncing experience to check whether you have subsequently joined Teams.

Learn more about how we process your information in connection with the contact syncing feature offered to Teams users.

If you do choose to join Teams, you will appear as a suggested new Teams contact for any Teams users with your information in their device, Outlook, or Skype address books. As a Teams user, you will be able to block other Teams users if you do not want to receive their

communications; additionally, you can report a concern to Microsoft.

Third-party contacts. You can also choose to sync contacts from third-party providers. If you choose to unsync your third-party contacts on Teams, all third-party contacts are deleted from Teams. If you gave your consent to use those third-party contacts on other Microsoft apps and services, these contacts will still be available to those other Microsoft apps and services.

You can remove third-party contacts from all Microsoft apps and services by removing third-party accounts from Teams. Please note that removing a third-party account from Teams may impact your experiences on other Microsoft apps and services that also use that third-party account.

Teams calendar. You can also choose to sync your Teams calendar with calendars from third-party providers. You can stop syncing your Teams calendar anytime by removing a third-party account from Teams. If you have consented to use third-party data on other

Microsoft apps and services, please note that removing this third-party account data in Teams may impact your experiences on other Microsoft apps and services.

Location sharing. You can share your static or live location with individuals or groups within Teams. You are in control and can stop sharing at any time. Sharing location for children is permitted with parental consent and in groups where an adult from the Microsoft family group is present.

Push notifications. To let you know of incoming calls, chats, and other messages, Teams uses the notification service on your device. For many devices, these services are provided by another company. To tell you who is calling, for example, or to give you the first few words of the new chat, Teams has to tell the notification service so that they can provide the notification to you. The company providing the notification service on your device will use this information in accordance with their own terms and privacy policy. Microsoft is not responsible for the data

collected by the company providing the notification service.

If you do not want to use the notification services for incoming Teams calls and messages, turn it off in the settings found on your device.

OneDrive

OneDrive lets you store and access your files on virtually any device. You can also share and collaborate on your files with others. Some versions of the OneDrive application enable you to access both your personal OneDrive by signing in with your personal Microsoft account and your OneDrive for Business by signing in with your work or school Microsoft account as part of your organization's use of Microsoft 365 or Office 365.

When you use OneDrive, we collect data about your usage of the service, as well as the content you store, to provide, improve, and protect the services. Examples include indexing the contents of your OneDrive documents so that you can search for them

later and using location information to enable you to search for photos based on where the photo was taken. We also collect device information so we can deliver personalized experiences, such as enabling you to sync content across devices and roam customized settings.

When you store content in OneDrive, that content will inherit the sharing permissions of the folder in which you store it. For example, if you decide to store content in the public folder, the content will be public and available to anyone on the internet who can find the folder. If you store content in a private folder, the content will be private.

When you share content to a social network like Facebook from a device that you have synced with your OneDrive account, your content is either uploaded to that social network, or a link to that content is posted to that social network. Doing this makes the content accessible to anyone on that social network. To delete the content, you need to delete it from the social network (if it was

uploaded there, rather than a link to it) and from OneDrive.

When you share your OneDrive content with your friends via a link, an email with the link is sent to those friends. The link contains an authorization code that allows anyone with the link to access your content. If one of your friends sends the link to other people, they will also be able to access your content, even if you did not choose to share the content with them. To revoke permissions for your content on OneDrive, sign in to your account and then select the specific content to manage the permission levels. Revoking permissions for a link effectively deactivates the link. No one will be able to use the link to access the content unless you decide to share the link again.

Files managed with OneDrive for Business are stored separately from files stored with your personal OneDrive. OneDrive for Business collects and transmits personal data for authentication, such as your email address and password, which will be transmitted to

Microsoft and/or to the provider of your Microsoft 365 or Office 365 service.

Outlook

Outlook products are designed to improve your productivity through improved communications and include Outlook.com, Outlook applications, and related services.

Outlook.com. Outlook.com is the primary consumer email service from Microsoft and includes email accounts with addresses that end in outlook.com, live.com, hotmail.com, and msn.com. Outlook.com provides features that let you connect with your friends on social networks. You will need to create a Microsoft account to use Outlook.com.

When you delete an email or item from a mailbox in Outlook.com, the item generally goes into your Deleted Items folder where it remains for approximately 7 days unless you move it back to your inbox, you empty the folder, or the service empties the folder automatically, whichever comes first. When the Deleted Items folder is emptied, those

emptied items remain in our system for up to 30 days before final deletion, unless we are legally required to retain the data for longer.

Outlook applications. Outlook client applications are software you install on your device that permits you to manage email, calendar items, files, contacts, and other data from email, file storage, and other services, like Exchange Online or Outlook.com, or servers, like Microsoft Exchange. You can use multiple accounts from different providers, including third-party providers, with Outlook applications.

To add an account, you must provide permission for Outlook to access data from the email or file storage services.

When you add an account to Outlook, your mail, calendar items, files, contacts, settings and other data from that account will automatically sync to your device. If you are using the mobile Outlook application, that data will also sync to Microsoft servers to enable additional features such as faster search, personalized filtering of less important mail,

and an ability to add email attachments from linked file storage providers without leaving the Outlook application. If you are using the desktop Outlook application, you can choose whether to allow the data to sync to our servers. At any time, you can remove an account or make changes to the data that is synced from your account.

If you add an account provided by an organization (such as your employer or school), the owner of the organizational domain can implement policies and controls (for example, requiring multi-factor authentication or the ability to remotely wipe data from your device) that can affect your use of Outlook.

To learn more about the data the Outlook applications collect and process, please see the Microsoft 365 section of this privacy statement.

Skype

Skype lets you send and receive voice, video, SMS, and instant message communications.

This section applies to the consumer version of Skype; if you are using Skype for Business, see the Enterprise and developer products section of this privacy statement.

As part of providing these features, Microsoft collects usage data about your communications that includes the time and date of the communication and the numbers or user names that are part of the communication.

Skype profile. Your Skype profile includes information you provided when you set up a Microsoft account. To enable other people to find you on Skype (or products that interact with Skype, such as Skype for Business), depending on your profile settings, your Skype profile is included in the Skype public search. Your profile includes your user name, avatar, and any other data you choose to add to your profile or display to others.

Emergency calling in the United States. If you enable location sharing for emergency calling, your location will be periodically collected to enable Microsoft to share your location with

emergency calling service providers if you dial 911. Your location information is only shared if you enable location sharing for emergency calling and you initiate a 911 call.

Skype contacts. If you use Outlook.com to manage contacts, Skype will automatically add the people you know to your Skype contact list until you tell the application to stop. With your permission, Skype will sync your device contacts periodically and check for other Skype users that match contacts in your device or Outlook address books. You are always in control of your contacts and can stop syncing at any time. You can block users if you do not want to receive their communications. If you choose to stop syncing your device contacts, or you are inactive on your device, any contacts that have not been matched during the synchronization process will be deleted from Skype. If you wish to invite any of your device or Outlook contacts to join a conversation, you can invite users to a 1:1 directly, or Microsoft can send an invitation on your behalf via SMS or email for invitations to group conversations. You can block users if

you do not want to receive their communications; additionally, you can report a concern to Microsoft.

Notice to non-user contacts. If your information appears in the device or Outlook address book of a Skype user who chooses to sync their device or Outlook contacts with their Skype contacts, Microsoft may process your data in order to determine whether you are a current Skype user and to allow Skype users to invite you to the service, including via SMS and email. As long as the Skype user continues to be active on Skype on their device and continues to enable contact syncing, your information will be stored on our servers and we will periodically process your information as a part of the Skype user's contact synching experience to check whether you have subsequently joined Skype.

Learn more about how we process your information in connection with the contact syncing feature offered to Skype users.

If you do choose to join Skype, you will appear as a suggested new Skype contact for any

Skype users with your information in their device or Outlook address books. As a Skype user, you will be able to block other Skype users if you do not want to receive their communications; additionally, you can report a concern to Microsoft.

Partner companies. To make Skype available to more people, we partner with other companies to allow Skype to be offered via those companies' services. If you use Skype through a company other than Microsoft, that company's privacy policy governs how it handles your data. To comply with applicable law or respond to valid legal process, or to help our partner company or local operator comply or respond, we may access, transfer, disclose, and preserve your data. That data could include, for example, your private content, such as the content of your instant messages, stored video messages, voicemails, or file transfers.

Skype Manager. Skype Manager lets you manage a group's (such as your family's) Skype usage from one central place. When you

set up a group, you will be the Skype Manager Administrator and can see the patterns of usage, including detailed information, like traffic data and details of purchases, of other members of the group who have consented to such access. If you add information like your name, other people in the group will be able to see it. Members of the group can withdraw consent for Skype Manager by visiting their Skype account page.

Push notifications. To let you know of incoming calls, chats, and other messages, Skype apps use the notification service on your device. For many devices, these services are provided by another company. To tell you who is calling, for example, or to give you the first few words of the new chat, Skype has to tell the notification service so that they can provide the notification to you. The company providing the notification service on your device will use this information in accordance with their own terms and privacy policy. Microsoft is not responsible for the data collected by the company providing the notification service. If you do not want to use

the notification services for incoming Skype calls and messages, turn it off in the settings found in the Skype application or your device.

Translation features. When you use Skype's translation features, Skype collects and uses your conversation to provide the translation service. With your permission, your data may be used to help improve Microsoft products and services. To help the translation and speech recognition technology learn and grow, sentences and automatic transcripts are analyzed and any corrections are entered into our system, to build better performing services. This data may include manual transcription of your voice clips. To learn more about how Microsoft manages your voice data, see Speech recognition technologies.

Recording features. Some versions of Skype have a recording feature that allows you to capture and share all or part of your audio / video call. The recording will be stored and shared as part of your conversation history with the person or group with whom the call occurred. **You should understand your legal**

responsibilities before recording any communication. This may include obtaining the prior consent of everyone participating in the conversation or any other authorizations as required. Microsoft is not responsible for how you use your recordings or the recording features.

Skype bots. Bots are programs offered by Microsoft or third parties that can do many useful things like search for news, play games, and more. Depending on their capabilities, bots may have access to your display name, Skype ID, country, region, language, and any messages, audio, video, or content that you share with the bot. Please review the bot profile and its privacy statement before engaging in a one-to-one or group conversation with a bot. You can delete a bot that you no longer wish to engage with. Prior to adding a bot to a group, please ensure that your group participants have consented to their information being shared with the bot.

Captioning. Certain Skype features include accessibility functionality such as captioning.

During Skype calls, a call participant can activate a voice-to-text feature, which allows the user to view the audio chat as text. If a user activates this feature, other call participants will not receive a notification. Microsoft uses this voice and text data to provide captioning of audio for users.

Surface Duo

The Surface Duo is a device featuring two screens that fits in your pocket for productivity on the go. Powered by the Google Android operating system, Surface Duo supports cellular and Wi-Fi connectivity and can be used for email, internet browsing, games, and business connectivity.

Microsoft provides a core Surface Duo experience that runs on the Android operating system. The core Surface Duo experience includes apps such as the Microsoft Launcher, Setup Wizard, and Your Phone Companion. You can sign in with a Google ID and enable various Google services; you can then also sign in with your Microsoft account (MSA) and enable Microsoft’s services. Microsoft apps

and services may rely on information provided by Google. Some features, such as location, require that you enable this functionality for Google and separately allow Microsoft to leverage this information.

Diagnostic data. Surface Duo collects diagnostic data to solve problems and to keep the core Surface Duo experience up to date, secure, and operating properly. This data also helps us improve Surface Duo and related Microsoft products and services. The data does not include your user name, email address, or the content of your files. There are two levels of diagnostic data: Required diagnostic data and Optional diagnostic data.

- **Required**. The minimum data necessary to help keep the core Surface Duo experience secure, up to date, and performing as expected.
- **Optional**. Additional data that helps us make product improvements and provides enhanced information to help Microsoft detect, diagnose, and remediate issues.

Learn more in Surface Duo Privacy Settings.

Surface Duo location settings. Surface Duo relies on Google location services to determine the device's precise geographic location to display the local weather. The location of your Surface Duo can be determined with varying degrees of accuracy and may in some cases be determined precisely. If you want Microsoft apps to be able to reference or display weather or other location related information, you need to enable Google location services and Microsoft location access. Some apps may require these settings be enabled independently for the app and can be set or changed in the Surface Duo's Settings. The Google Privacy Policy provides details about Google's location service and related data privacy practices. See Surface Duo Location Settings for more information.

Microsoft apps included with the Surface Duo. The diagnostic data options for the core Surface Duo experience are configured when you initially set up your Surface Duo and can be changed in the Surface Duo's Settings under the Diagnostic Data section.

The other Microsoft apps on your Surface Duo may prompt you to enable functionality to enable the full experience of the app or you may be asked to allow optional diagnostic data collection. You can change the settings for these apps in the Surface Duo Settings under the app name. More information about these apps is available in the Productivity and communications products and Search, Microsoft Edge, and artificial intelligence sections of this Privacy Statement.

LinkedIn

To learn about the data LinkedIn collects and how it is used and shared, please see LinkedIn's Privacy Policy.

Search, Microsoft Edge, and artificial intelligence

Search and artificial intelligence products connect you with information and intelligently sense, process, and act on information—learning and adapting over time.

Bing

Bing services include search and mapping services, as well as other apps and programs described in this section. Bing services collect and process data in many forms, including text that has been inked or typed, voice data, and images. Bing services are also included within other Microsoft services, such as Microsoft 365, Cortana, and certain features in Windows (which we refer to as Bing-powered experiences).

When you conduct a search, or use a feature of a Bing-powered experience that involves conducting a search or entering a command on your behalf, Microsoft will collect the searches or commands you provide (which may be in the form of text, voice data, or an image), along with your IP address, location, the unique identifiers contained in our cookies or similar technologies, the time and date of your search, and your browser configuration. For example, if you use Bing voice-enabled services, your voice input and performance data associated with the speech functionality will be sent to Microsoft. To learn more about

how Microsoft manages your voice data, see Speech recognition technologies. And, if you use Bing image-enabled services, the image you provide will be sent to Microsoft. When you use Bing-powered experiences, such as Bing Lookup to search a particular word or phrase within a webpage or document, that word or phrase is sent to Bing along with some surrounding content in order to provide contextually relevant search results.

AI-powered Bing search. Bing search now includes an AI-enhanced web search functionality, Bing Chat, which supports users by providing relevant search results, reviewing and summarizing from across the web, refining research queries through the chat experience, and sparking creativity by helping users create content. Bing Chat's use and collection of personal data is consistent with Bing's core web search offering as described in this section. More information about the new Bing experience is available at The New Bing: Our approach to Responsible AI.

Search suggestions. For the search suggestions feature, the characters that you type into a Bing-powered experience (such as search and site suggestions in the Microsoft Edge browser) to conduct a search and what you click on will be sent to Microsoft. This allows us to provide you with relevant suggestions as you type your searches. To turn this feature on or off, while using Bing Search, go to Bing Settings. There are other methods to control this feature in other Bing-powered experiences, such as the Microsoft Edge browser. Search Suggestions cannot be turned off in the search box in Windows 10 and Windows 11. If you choose, you can always hide the search box or icon on the taskbar.

Bing experience improvement program for Bing Desktop and Bing Toolbar. If you are using Bing Desktop or Bing Toolbar and choose to participate in the Bing Experience Improvement Program, we also collect additional data about how you use these specific Bing apps, such as the addresses of the websites you visit, to help improve search

ranking and relevance. To help protect your privacy, we do not use the data collected through the Bing Experience Improvement Program to identify or contact you or target advertising to you. You can turn off the Bing Experience Improvement Program at any time in the Bing Desktop or Bing Toolbar settings. Finally, we delete the information collected through the Bing Experience Improvement Program after 18 months.

Retention and de-identification. We de-identify stored search queries by removing the entirety of the IP address after 6 months, and cookie IDs and other cross-session identifiers that are used to identify a particular account or device after 18 months.

Personalization through Microsoft account. Some Bing services provide you with an enhanced experience when you sign in with your personal Microsoft account, for example, syncing your search history across devices. You can use these personalization features to customize your interests, favorites, and settings, and to connect your account with

third-party services. Visit Bing Settings to manage your personalization settings, or the Microsoft privacy dashboard to manage your data.

Managing search history. When you're signed-in to a personal Microsoft account, you can erase your search and chat history on the Microsoft privacy dashboard. The Search History service from Bing, located in Bing Settings, provides another method of revisiting the search terms you've entered and results you've clicked when using Bing search through your browser. You may clear your search history on a device through this service. The conversations you have with Bing chat are also remembered as "Recent activity". The history of previous Recent activities is saved, with the names of chats based by default on the first query of the chat. Your Recent activity is displayed on the right-hand side of the chat window when you are using the service. Clearing your history prevents that history from being displayed in your Search History or chat history, but does not delete information from our search logs, which are retained and de-

identified as described above or as you have instructed through the privacy dashboard. If you are signed-in to a work or school Microsoft account using Microsoft Search in Bing, you can export your Microsoft Search in Bing search history, but you cannot delete it. Your Microsoft Search in Bing service administrator can see aggregated search history across all enterprise users but cannot see specific searches by user. However, if you are using Bing Chat for Enterprise while signed-in to a work or school Microsoft account, your Bing Chat for Enterprise conversations will not be saved or stored.

Third-party services that use Bing. You may access Bing-powered experiences when using third-party services, such as those from Yahoo!. In order to provide these services, Bing receives data from these and other partners, including your search query and related data (such as date, time, IP address, and a unique identifier). This data will be sent to Microsoft to provide the search service. Microsoft will use this data as described in this statement or as further limited by our contractual

obligations with our partners. You should refer to the privacy policies of the third-party services for any questions about how they collect and use data.

Data passed to destination website. When you select a search result or advertisement from a Bing search results page and go to the destination website, the destination website will receive the standard data your browser sends to every web site you visit—such as your IP address, browser type and language, and the host name of the site you came from (in this case, https://www.bing.com/).

Sharing data from Bing and Bing-powered experiences with third parties. We share some de-identified data (data where the identity of a specific person is not known) from Bing and Bing-powered experiences with selected third parties. Before we do so, we run the data through a process designed to remove certain sensitive data that users may have included in the search terms themselves (such as social security numbers or credit card numbers). Additionally, we require these third parties to

keep the data secure and to not use the data for purposes other than for which it is provided.

Cortana

Cortana is your personal productivity assistant in Microsoft 365. As a digital assistant, Cortana is designed to help you achieve more with less effort so you can focus on what matters and can answer a wide range of questions about things such as weather, sports, stocks, and general information. When you ask questions, the data Cortana collects depends on whether you are using the consumer or enterprise version.

This section applies to the consumer version of Cortana experiences in Windows 10 and Windows 11. If you are using Cortana with an account provided by an organization, such as a work or school account, see the Notice to end users section of this privacy statement. Learn more about the enterprise version of Cortana in Microsoft 365.

When you ask Cortana a question, whether you are speaking or typing, Cortana collects that question as a text string. To answer your questions Cortana uses the Bing service. For information about the data Bing collects, see the Bing section of this privacy statement.

By default, if you speak your question, Cortana also collects speech transcription data and does not collect voice clips. You have the option to provide your consent and allow Microsoft to collect voice clips. If you choose to opt in and allow Microsoft to collect voice clips, the voice clip files are stored and anonymized and will not be associated with your Microsoft account or any other Microsoft IDs. This anonymous data is used to improve the product. For more information about Microsoft and your voice data, see the Speech Recognition Technologies section of this privacy statement.

Cortana legacy. Cortana in Windows 10 version 1909 and earlier collects user query data (a text transcription of the question the user asked), which is anonymized and used for

product maintenance. Cortana in Windows 10 version 1909 also uses the Bing service to answer your questions. For information about the data Bing collects, see the Bing section of the Privacy Statement.

Learn more about Cortana and privacy.

Microsoft Edge

Whenever you use a web browser to access the internet, data about your device ("standard device data") is sent to the websites you visit and online services you use. Standard device data includes your device's IP address, browser type and language, access times, and referring website addresses. This data might be logged on those websites' or online services' web servers. Which data is logged and how that data is used depends on the privacy practices of the websites you visit and web services you use. Certain features in Microsoft Edge, such as when you open a new tab in the browser, connect you to Microsoft Start Content and your experiences with such content is covered by the Microsoft Start section of this privacy statement. Additionally,

Microsoft Edge sends a unique browser ID to certain websites to enable us to develop aggregate data used to improve browser features and services.

Microsoft Edge for Windows, Linux, and macOS. Microsoft Edge is the default web browser for Windows 10 and later and is also available on other supported versions of Windows and macOS.

Data about how you use your browser, such as your browsing history, web form data, temporary internet files, and cookies, is stored on your device. You can delete this data from your device using Clear Browsing History.

Microsoft Edge allows you to capture and save content on your device, such as:

- **Settings and More**. Allows you to manage your favorites, downloads, history, extensions, and collections.
- **Collections**. Allows you to collect text, images, videos, and other content in a note page in your browser. When you drag content into your collection, it is cached on

your device and can be deleted through your collection.
- **Website Pin to Taskbar**. Allows you to pin your favorite websites to the Windows taskbar. Websites will be able to see which of their webpages you have pinned, so they can provide you a notification badge letting you know there is something new for you to check out on their websites.

Microsoft collects data necessary to provide features you request in Microsoft Edge. When signed into Microsoft Edge using your Microsoft personal account or work or school account, Microsoft Edge will sync your browser data saved on your device across other signed-in devices. You may choose which browser data to sync, including your favorites, browsing history, extensions and associated data, settings, open tabs, autofill form entries (such as your name, address, and phone number), passwords, payment information, and other data types as they become available. If you choose to sync extensions that you acquired from third-party web stores, a copy of those extensions will be

downloaded directly from those web stores on your synced device(s). If you have turned on Password Monitor, your saved credentials are hashed, encrypted and sent to Microsoft's Password Monitor service to warn you if your credentials were detected as part of a malicious attack or a breach. Microsoft does not retain this data after the check is complete. You can disable or configure syncing in the Microsoft Edge settings.

When you sign into Microsoft Edge with your Microsoft personal account or work or school account, Microsoft Edge will store your account's privacy preferences. Microsoft Edge will use the stored preferences to migrate your account's privacy choices across your signed-in devices, including during Windows device set up or when you sign into Microsoft Edge with your account on a new device.

Microsoft Edge's **Search and site suggestions** uses your search queries and browsing history to provide you with faster browsing and more relevant search recommendations. Microsoft Edge sends the information you type into the

browser address bar to the default search provider configured in the address bar to offer search recommendations as you type each character. You can turn off these features at any time in the browser settings. In order to provide search results, Microsoft Edge sends your search queries, standard device information, and location (if you have location enabled) to your default search provider. If Bing is your default search provider, we use this data as described in the Bing section of this privacy statement.

Microsoft Edge collects and uses data from your search activity across the web, including websites Microsoft does not own or operate, to improve Microsoft services, such as Microsoft Edge, Microsoft Bing and Microsoft News. This data may include the search query, the search results that are displayed to you, demographic information that is part of the search results, and the interaction you have with those search results, such as the links you click. Microsoft Edge takes steps to de-identify the data it collects by removing data that identifies the person or device from which it

was collected and retains this data for one year from when it is collected. Microsoft does not use this collected data to personalize or provide ads to you. You can turn off the collection of this data at any time in the browser settings.

Microsoft Edge downloads content from Microsoft services to enhance your browsing experiences; for example, when data is downloaded to prerender site content for faster browsing or to provide content required to power features you choose to use, such as providing templates for Collections.

You may also choose to share your Microsoft Edge browsing activity to allow us to personalize Microsoft Edge and Microsoft services like ads, search, shopping, and news. Microsoft Edge browsing activity includes your history, favorites, usage data, web content, and other browsing data. For more information about our **advertising privacy policies** see the Advertising section of the privacy statement. In the Microsoft privacy dashboard you can control the use of your browsing activity for

personalized ads in the **See ads that interest you** setting. If you disable this setting in the Microsoft privacy dashboard you will continue to receive personalized web experiences like search and news based on your browsing activity. You may stop sharing your Microsoft Edge browsing activity by disabling **Allow Microsoft to use your browsing activity including history, favorites, usage and other browsing data to personalize Microsoft Edge and Microsoft services like ads, search, shopping and news** within Edge settings. When using Bing chat features in the Microsoft Edge sidebar, you can choose to allow Bing to access the content of the webpage you are viewing in order to provide further insights, such as page summaries. Use of data connected with Bing conversational experiences is described in the Bing section of this privacy statement.

Microsoft Edge collects required diagnostic data to solve problems and to keep Microsoft Edge up to date, secure, and operating properly. Required diagnostic data also helps us improve Microsoft Edge and Windows.

Separate from your search activity data mentioned above, you can choose to send optional diagnostic data about how you use Microsoft Edge and information about your browser activity, including browsing history and search terms to Microsoft to help us improve Microsoft Edge and other Microsoft products and services. For Microsoft Edge on Windows 10 and later, this information is provided when you have enabled optional diagnostic data. For details, see the Windows Diagnostics section of the privacy statement. For Microsoft Edge on other operating systems, optional diagnostic information is provided when you enable **Improve Microsoft products by sending data about how you use the browser** or **Make searches and Microsoft products better by sending info about websites you visit in Microsoft Edge** in the browser settings.

The diagnostic data collected by Microsoft Edge is transmitted to Microsoft and is stored with one or more unique identifiers that help us recognize an individual browser installation

on a device and understand the browser's service issues and use patterns.

Learn more about Microsoft Edge, browsing data, and privacy.

Microsoft Edge on iOS and Android. Microsoft Edge on iOS and Android devices collects data necessary to provide features you request in Microsoft Edge. Microsoft also collects required diagnostic data to solve problems and to keep Microsoft Edge up to date, secure, and operating properly. Required diagnostic data also helps us improve Microsoft Edge.

Additionally, you may share optional diagnostic data about how you use Microsoft Edge and information about websites you visit (browsing history) for personalized experiences on your browser, Windows, and other Microsoft products and services. This information also helps us improve Microsoft Edge and other Microsoft products and services. This optional diagnostic data is sent to us when you enable **Share usage data for personalization** or **Share info about websites you visit** in the browser settings.

The diagnostic data collected by Microsoft Edge is transmitted to Microsoft and is stored with one or more unique identifiers that help us recognize an individual user on a device and understand the browser's service issues and use patterns.

Microsoft Edge uses data from your search activity across the web, including search activity on websites Microsoft does not own or operate, to improve Microsoft services like Microsoft Edge, Microsoft Bing, and Microsoft News. The data Microsoft Edge collects may include personal data; however, Microsoft Edge takes steps to scrub and de-identify the data. Microsoft Edge does not use this data to personalize or provide ads for you. You can turn off the collection of this data at any time in the browser settings. Learn more about Search results data for product improvement.

For information about the privacy practices of legacy versions Microsoft Edge (versions 44 and below), see the Web browsers—Microsoft Edge Legacy and Internet Explorer section of the privacy statement.

Microsoft Translator

Microsoft Translator is a machine translation system and service designed to automatically translate text and voice input between numerous supported languages. Microsoft Translator is made available as a stand-alone consumer app for Android, iOS, and Windows and its service capabilities are also integrated in a variety of Microsoft products and services, such as Translator Hub, Translator for Bing, and Translator for Microsoft Edge. Microsoft Translator processes the text, image, and voice data you submit, as well as device and usage data. We use this data to provide Microsoft Translator, personalize your experiences, and improve our products and services. Microsoft has implemented business and technical measures designed to help de-identify the data you submit to Microsoft Translator. For example, when we randomly sample text and audio to improve Microsoft Translator and Microsoft’s speech recognition technologies, we delete identifiers and certain text, such as email addresses and some

number sequences, detected in the sample that could contain personal data. To learn more about how Microsoft manages your voice data, see Speech recognition technologies.

Separate from Microsoft Translator, Microsoft translation services are available as features in other Microsoft products and services that have different privacy practices than Microsoft Translator. For more information on the Microsoft Azure Cognitive Services Translator Text API, Custom Translator, and Translator Speech API, see the Enterprise and developer products section of this privacy statement. For the Translate feature in Microsoft 365 apps and Skype, see the Productivity and communications products section of this privacy statement.

SwiftKey

The Microsoft Swiftkey keyboard and related cloud-based services (collectively, the "SwiftKey Services") process data about words you use and how you type and use this data to learn your writing style and provide

personalized autocorrection and predictive text that adapts to you. We also use this data to offer a range of other features, such as hashtag and emoji predictions.

SwiftKey prediction technology learns from the way you use language to build a personalized language model. This model is an optimized view of the words and phrases that you use most often in context and reflects your unique writing style. The model itself contains the words you commonly type arranged in a way that enables SwiftKey's algorithms to make predictions, based on text you have already entered. The model draws from all scenarios in which you use your keyboard, including when you type while using apps or visiting websites. The SwiftKey keyboard and model attempt to avoid collecting sensitive data, by not collecting data from certain fields such as those recognized as containing password or payment data. SwiftKey Services do not log, store, or learn from data you type, or the data contained in your model, unless you choose to share your data with us (as described further below). When you use SwiftKey Services, we

also collect device and usage data. We use de-identified device and usage data to analyze service performance and help improve our products.

The SwiftKey Services also include an optional cloud component called a SwiftKey Account. If you choose to create a SwiftKey Account, your language model will be synced with the SwiftKey Account cloud service, so you can benefit from that model on the different devices you use and access additional services such as prediction synchronization and backup. When you create a SwiftKey Account, Microsoft will also collect your email address and basic demographic data. All data collected is transferred to our servers over encrypted channels.

You may also opt in to share your language, typing data, and/or voice clips for the purposes of improving Microsoft products and services. Depending on the opt-ins you choose, SwiftKey may send short snippets of data about what and how you type and/or your voice clips, and related correction data to our

servers for processing. These text snippets and/or voice clips are used in various automated processes to validate that our prediction services are working correctly and to make product improvements. To preserve your privacy, SwiftKey Services de-identify these text snippets, and even if you have a SwiftKey Account, these text snippets and/or voice clips will not be linked to it. To learn more about how Microsoft manages your voice data, see Speech recognition technologies.

If you sign into your SwiftKey Account and opt to share your language and typing data or voice clips, Microsoft will process your shared data in order to look for new patterns of language usage across our user base. This allows us to improve our basic models for individual languages. Language and typing data used in this process is aggregated and any words or combinations of words that might be personal to individuals or small groups of users are filtered out.

You can withdraw your consent to share your language and typing data or voice clips for product improvement at any time in SwiftKey Settings. You can also withdraw your consent for SwiftKey Services to retain your personal data in SwiftKey Settings. When you withdraw consent for SwiftKey to retain your personal data, all personal data collected through your use of the SwiftKey Services will be deleted.

You may receive occasional notifications on your device alerting you to product updates and features that may be of interest to you. You can disable these notifications at any time in the SwiftKey Settings.

Windows

Windows is a personalized computing environment that enables you to seamlessly roam and access services, preferences, and content across your computing devices from phones to tablets to the Surface Hub. Rather than residing as a static software program on your device, key components of Windows are cloud-based, and both cloud and local elements of Windows are updated regularly, providing you with the latest

improvements and features. In order to provide this computing experience, we collect data about you, your device, and the way you use Windows. And because Windows is personal to you, we give you choices about the personal data we collect and how we use it. Note that if your Windows device is managed by your organization (such as your employer or school), your organization may use centralized management tools provided by Microsoft or others to access and process your data and to control device settings (including privacy settings), device policies, software updates, data collection by us or the organization, or other aspects of your device. Additionally, your organization may use management tools provided by Microsoft or others to access and process your data from that device, including your interaction data, diagnostic data, and the contents of your communications and files. For more information about data collection in Windows, see Data collection summary for Windows. This statement discusses Windows 10 and Windows 11 and references to Windows in this section relate to those product versions. Earlier versions of Windows (including Windows Vista, Windows 7,

Windows 8, and Windows 8.1) are subject to their own privacy statements.

Activation

When you activate Windows, a specific product key is associated with the device on which your software is installed. The product key and data about the software and your device is sent to Microsoft to help validate your license to the software. This data may be sent again if there is a need to re-activate or validate your license. On phones running Windows, device and network identifiers, as well as device location at the time of the first power-up of the device, are also sent to Microsoft for the purpose of warranty registration, stock replenishment, and fraud prevention.

Activity history

Activity history helps keep track of the things you do on your device, such as the apps and services you use, the files you open, and the websites you browse. Your activity history is created when using different apps and

features such as Microsoft Edge Legacy, some Microsoft Store apps, and Microsoft 365 apps and is stored locally on your device. If you've signed in to your device with a work or school account and give your permission, Windows sends your activity history to Microsoft. Once your activity history is in the cloud, Microsoft uses that data to enable cross-device experiences, to provide you with the ability to continue those activities on other devices, to provide personalized experiences (such as ordering your activities based on duration of use) and relevant suggestions (such as anticipating what your needs might be based on your activity history), and to help improve Microsoft products.

You can turn settings off or on for sending your activity history to Microsoft and storing activity history locally on your device, and you can also clear your device's activity history at any time by going to **Privacy > Activity history** in the Windows settings app. Learn more about activity history in Windows.

Advertising ID

Windows generates a unique advertising ID for each person using a device, which app developers and advertising networks can then use for their own purposes, including providing relevant advertising in apps. When the advertising ID is enabled, both Microsoft apps and third-party apps can access and use the advertising ID in much the same way that websites can access and use a unique identifier stored in a cookie. Thus, your advertising ID can be used by app developers and advertising networks to provide more relevant advertising and other personalized experiences across their apps and on the web. Microsoft collects the advertising ID for the uses described here only when you choose to enable the advertising ID as part of your privacy setting.

The advertising ID setting applies to Windows apps using the Windows advertising identifier. You can turn off access to this identifier at any time by turning off the advertising ID in the Windows settings app. If you choose to turn it on again, the advertising ID will be reset and a new identifier will be generated. When a third-

party app accesses the advertising ID, its use of the advertising ID will be subject to its own privacy policy. Learn more about advertising ID in Windows.

The advertising ID setting does not apply to other methods of interest-based advertising delivered by Microsoft or third parties, such as cookies used to provide interest-based display ads on websites. Third-party products accessed through or installed on Windows may also deliver other forms of interest-based advertising subject to their own privacy policies. Microsoft delivers other forms of interest-based ads in certain Microsoft products, both directly and by partnering with third-party ad providers. For more information on how Microsoft uses data for advertising, see the How we use personal data section of this statement.

Diagnostics

Microsoft collects Windows diagnostic data to solve problems and to keep Windows up to date, secure, and operating properly. It also helps us improve Windows and related

Microsoft products and services and, for customers who have turned on the “Tailored experiences” setting, to provide more relevant tips and recommendations to tailor Microsoft and third-party products and services for Windows to the customer’s needs. This data is transmitted to Microsoft and stored with one or more unique identifiers that can help us recognize an individual user on an individual device and understand the device's service issues and use patterns.

There are two levels of diagnostic and activity data: Required diagnostic data and Optional diagnostic data. Certain product documentation and other materials refer to Required diagnostic data as Basic diagnostic data and to Optional diagnostic data as Full diagnostic data.

If an organization (such as your employer or school) uses Azure Active Directory (AAD) to manage the account it provides to you and enrolls your device in the Windows diagnostic data processor configuration, Microsoft’s processing of diagnostic data in connection

with Windows is governed by a contract between Microsoft and the organization. If an organization uses Microsoft management tools or engages Microsoft to manage your device, Microsoft and the organization will use and process diagnostic and error data from your device to allow the management, monitoring, and troubleshooting of your devices managed by the organization, and for other purposes of the organization.

Required diagnostic data includes information about your device, its settings and capabilities, and whether it is performing properly. We collect the following Required diagnostic data:

- Device, connectivity, and configuration data:
  - Data about the device such as the processor type, OEM manufacturer, type of battery and capacity, number and type of cameras, firmware, and memory attributes.
  - Network capabilities and connection data such as the device's IP address, mobile network (including IMEI and

mobile operator), and whether the device is connected to a free or paid network.
    - Data about the operating system and its configuration such as the OS version and build number, region and language settings, diagnostics data settings, and whether the device is part of the Windows Insider program.
    - Data about connected peripherals such as model, manufacturer, drivers, and compatibility data.
    - Data about the applications installed on the device such as application name, version, and publisher.
- Whether a device is ready for an update and whether there are factors that may impede the ability to receive updates, such as low battery, limited disk space, or connectivity through a paid network.
- Whether updates complete successfully or fail.
- Data about the reliability of the diagnostics collection system itself.
- Basic error reporting, which is health data about the operating system and

applications running on your device. For example, basic error reporting tells us if an application, such as Microsoft Paint or a third-party game, hangs or crashes.

Optional diagnostic data includes more detailed information about your device and its settings, capabilities, and device health. Optional diagnostic data also includes data about the websites you browse, device activity (also sometimes referred to as usage), and enhanced error reporting that helps Microsoft to fix and improve products and services for all users. When you choose to send Optional diagnostic data, Required diagnostic data will always be included, and we collect the following additional information:

- Additional data about the device, connectivity, and configuration, beyond that collected under Required diagnostic data.
- Status and logging information about the health of operating system and other system components beyond that collected about the update and diagnostics systems under Required diagnostic data.

- App activity, such as which programs are launched on a device, how long they run, and how quickly they respond to input.
- Browser activity, including browsing history and search terms, in Microsoft browsers (Microsoft Edge or Internet Explorer).
- Enhanced error reporting, including the memory state of the device when a system or app crash occurs (which may unintentionally contain user content, such as parts of a file you were using when the problem occurred). Crash data is never used for Tailored experiences as described below.

Some of the data described above may not be collected from your device even if you choose to send Optional diagnostic data. Microsoft minimizes the volume of Optional diagnostic data it collects from all devices by collecting some of the data from only a subset of devices (sample). By running the Diagnostic Data Viewer tool, you can see an icon which indicates whether your device is part of a sample and also which specific data is collected from your device. Instructions for

how to download the Diagnostic Data Viewer tool can be found in the Windows settings app under Diagnostics & feedback.

Specific data items collected in Windows diagnostics are subject to change to give Microsoft flexibility to collect the data needed for the purposes described. For example, to enable Microsoft to troubleshoot the latest performance issue impacting users' computing experience or update a Windows device that is new to the market, Microsoft may need to collect data items that were not collected previously. For a current list of data types collected at **Required diagnostic data** and **Optional diagnostic data**, see Windows Required (Basic level) diagnostic events and fields or Windows Optional (Full level) diagnostic data. We provide limited portions of error report information to partners (such as the device manufacturer) to help them troubleshoot products and services which work with Windows and other Microsoft product and services. They are only permitted to use this information to repair or improve those products and services. We may also

share some aggregated, de-identified diagnostic data, such as general usage trends for Windows apps and features, with selected third parties. Learn more about diagnostic data in Windows.

Inking and typing Recognition. You also can choose to help Microsoft improve inking and typing recognition by sending inking and typing diagnostic data. If you choose to do so, Microsoft will collect samples of the content you type or write to improve features such as handwriting recognition, autocompletion, next word prediction, and spelling correction in the many languages used by Microsoft customers. When Microsoft collects inking and typing diagnostic data, it is divided into small samples and processed to remove unique identifiers, sequencing information, and other data (such as email addresses and numeric values) which could be used to reconstruct the original content or associate the input to you. It also includes associated performance data, such as changes you manually make to text, as well as words you've added to the

dictionary. Learn more about improving inking and typing in Windows.

If you choose to turn on **Tailored experiences**, we will use your Windows diagnostic data (Required or Optional as you have selected) to offer you personalized tips, ads, and recommendations to enhance Microsoft experiences. If you have selected Required as your diagnostic data setting, personalization is based on information about your device, its settings and capabilities, and whether it is performing properly. If you have selected Optional, personalization is also based on information about how you use apps and features, plus additional information about the health of your device. However, we do not use information about the websites you browse, the content of crash dumps, speech, typing, or inking input data for personalization when we receive such data from customers who have selected Optional.

Tailored experiences include suggestions on how to customize and optimize Windows, as well as ads and recommendations for

Microsoft and third-party products and services, features, apps, and hardware for your Windows experiences. For example, to help you get the most out of your device, we may tell you about features you may not know about or that are new. If you are having a problem with your Windows device, you may be offered a solution. You may be offered a chance to customize your lock screen with pictures, or to be shown more pictures of the kind you like, or fewer of the ones you do not. If you stream movies in your browser, you may be recommended an app from the Microsoft Store that streams more efficiently. Or, if you are running out of space on your hard drive, Windows may recommend you try OneDrive or purchase hardware to gain more space. Learn more about tailored experiences in Windows.

Feedback Hub

Feedback Hub is a preinstalled app that provides a way to gather feedback on Microsoft products and installed first party and third-party apps. You can sign into Feedback Hub using either your personal

Microsoft account or an account provided by your organization (such as your employer or school) that you use to sign into Microsoft products. Signing in with your work or school account allows you to submit feedback to Microsoft in association with your organization.

Any feedback you provide whether using your work or school account or personal Microsoft account may be publicly viewable depending on the settings configured by your organization's administrators. Additionally, if feedback is provided using your work or school account, your feedback can be viewed through the Feedback Hub by your organization's administrators.

When you submit feedback to Microsoft about a problem or add more details to a problem, diagnostic data will be sent to Microsoft to improve Microsoft products and services. Depending on your Diagnostic data settings in the **Diagnostics & feedback** section of the Windows settings app, Feedback Hub will either send diagnostic data automatically or

you will have the option to send it to Microsoft at the time you provide feedback. Based on the category chosen when submitting feedback, there may be additional personal data collected that helps to further troubleshoot issues; for example, location related information when submitting feedback about location services or gaze related information when submitting feedback on Mixed Reality. Microsoft may also share your feedback along with the data collected when you submit your feedback with Microsoft partners (such as a device manufacturer, or firmware developer) to help them troubleshoot products and services that work with Windows and other Microsoft products and services. Learn more about diagnostic data in Windows.

Location services and recording

Windows location service. Microsoft operates a location service that helps determine the precise geographic location of a specific Windows device. Depending on the capabilities of the device, the device's location can be determined with varying degrees of

accuracy and may in some cases be determined precisely. When you have enabled location on a Windows device, or you have given permission for Microsoft apps to access location information on non-Windows devices, data about cell towers and Wi-Fi access points and their locations is collected by Microsoft and added to the location database after removing any data identifying the person or device from which it was collected. This de-identified location information is used to improve Microsoft's location services and, in some instances, shared with our location service provider partners, currently HERE (see https://www.here.com/) and Skyhook (see https://www.skyhook.com) to improve the location services of the provider.

Windows services and features, apps running on Windows, and websites opened in Windows browsers can access the device's location through Windows if your settings allow them to do so. Some features and apps request location permission when you first install Windows, some ask the first time you use the app, and others ask every time you access the

device’s location. For information about certain Windows apps that use the device’s location, see the Windows apps section of this privacy statement.

When an app or feature accesses the device’s location and you are signed in with a Microsoft account, your Windows device will also upload its location to the cloud where it is available across your devices to other apps or services that use your Microsoft account and for which you’ve granted permission. We will retain only the last known location (each new location replaces the previous one). Data about a Windows device's recent location history is also stored on the device even if not using a Microsoft account, and certain apps and Windows features can access this location history. You can clear your device's location history at any time in the Windows settings app.

In the Windows settings app, you can also view which apps have access to the device’s precise location or your device's location history, turn off or on access to the device’s

location for particular apps, or turn off access to the device's location. You can also set a default location, which will be used when the location service can't detect a more exact location for your device.

There are some exceptions to how your device's location can be determined that are not directly managed by the location settings.

Desktop apps are a specific type of app that won't ask for separate permission to discover your device location information and won't appear in the list that allows you to choose apps that can use your location. They can be downloaded from the Microsoft Store, downloaded from the internet, or installed with some type of media (such as a CD, DVD, or USB storage device). They're opened using an .EXE, .MSI, or .DLL file, and they typically run on your device, unlike web-based apps (which run in the cloud). Learn more about third-party desktop apps and how they may still be able to determine your device's location when the device's location setting is off.

Some web-based experiences or third-party apps that surface on Windows could use other technologies (such as Bluetooth, Wi-Fi, cellular modem, etc.) or cloud-based location services to determine your device's location with varying degrees of accuracy even when you've turned off the device location setting.

In addition, to facilitate getting help in an emergency, whenever you make an emergency call, Windows will attempt to determine and share your precise location, regardless of your location settings. If your device has a SIM card or is otherwise using cellular service, your mobile operator will have access to your device's location. Learn more about location in Windows.

General Location. If you turn on Location services, apps that cannot use your precise location may still have access to your general location, such as your city, postal code, or region.

Find my device. The Find my device feature allows an administrator of a Windows device to find the location of that device from

account.microsoft.com/devices. To enable Find my device, an administrator needs to be signed in with a Microsoft account and have the location setting enabled. This feature will work even if other users have denied access to location for all their apps. When the administrator attempts to locate the device, users will see a notification in the notification area. Learn more about Find my device in Windows.

Recording. Some Windows devices have a recording feature that allows you to capture audio and video clips of your activity on the device, including your communications with others. If you choose to record a session, the recording will be saved locally on your device. In some cases, you may have the option to transmit the recording to a Microsoft product or service that broadcasts the recording publicly. **Important: You should understand your legal responsibilities before recording and/or transmitting any communication. This may include obtaining the prior consent of everyone participating in the conversation or any other authorizations as required.**

Microsoft is not responsible for how you use recording features or your recordings.

Phone Link - Link to Windows

Phone Link - Link to Windows The Phone Link app lets you link your Android phone with your Microsoft Account, enabling a variety of cross-device experiences. You can use Phone Link to see recent photos from your Android phone on your Windows device; make and receive calls from your Android phone on your Windows device; view and send text messages from your Windows device; view, dismiss, or perform other actions to your Android phone notifications from your Windows device; share your phone screen on your Windows device through Phone Link’s mirroring function; and instantly access Android apps installed on your Android phone on your Windows device.

To use Phone Link, the Phone Link app must be installed on your Windows device and the Link to Windows app must be installed on your Android phone.

To use Phone Link, you must log into your Microsoft account on the Phone Link app on your Windows device and on the Link to Windows app on your Android phone. Your Android phone and your Windows device must be connected to the internet. Some features will require you to enable Bluetooth and pair your phone with your PC. To use the Calls feature, your Android phone must also have Bluetooth enabled.

During setting up your Windows device, you can choose to link your phone with your Microsoft account. This is done by signing into Link to Windows on your Android phone, granting permissions and completing the onboarding experience. Once complete, Link to Windows will sync your data, such as your text messages, contacts, call history, photos, notifications, and other information, to all your Windows PCs where you have signed into your Microsoft account. See below for details on how your data is used.

As part of providing Phone Link’s features to you, Microsoft collects performance, usage,

and device data that includes, for example, the hardware capabilities of your mobile phone and Windows device, the number and duration of your sessions on Phone Link, and the amount of time you spent during setup.

You can unlink your Android phone from your Windows device at any time by going into your Phone Link app settings and choosing to remove your Android phone. You can do the same from the app settings on the Link to Windows app on your Android phone. For detailed information, see our support page.

Text Messages. Phone Link allows you to view text messages delivered to your Android phone on your Windows device and send text messages from your Windows device. Only text messages received and sent within the last 30 days are visible on your Windows device. These text messages are temporarily stored on your Windows device. We never store your text messages on our servers or change or delete any text messages on your Android phone. You can see messages sent via SMS (Short Message Service) and MMS

(Multimedia Messaging Service) on Android devices, and messages sent via RCS (Rich Communication Services) on select Samsung devices on select mobile operator networks. To provide this functionality, Phone Link accesses the content of your text messages and the contact information of the individuals or businesses from whom you are receiving or sending text messages.

Calls. Phone Link allows you to make and receive calls from your Android phone on your Windows device. Through Phone Link, you can also view your recent calls on your Windows device. To activate this feature, you must enable certain permissions on both your Windows device and Android phone, such as call logs access and permission to make phone calls from your PC. These permissions can be revoked at any time under the Phone Link Settings page on your Windows device and your Android phone's settings. Only calls received and dialed within the last 30 days are visible under call logs on your Windows device. These call details are temporarily stored on

your Windows device. We do not change or delete your call history on your Android phone.

Photos. Phone Link allows you to copy, share, edit, save, or delete photos from your Android phone on your Windows device. Only a limited number of your most recent photos from the Camera Roll and Screenshots folders on your Android phone will be visible on your Windows device at any given time. These photos are temporarily stored on your Windows device and as you take more photos on your Android phone, we remove the temporary copies of the older photos from your Windows device. We never store your photos on our servers or change or delete any photos on your Android phone.

Notifications. Phone Link allows you to view your Android phone's notifications on your Windows device. Through Phone Link, you can read and dismiss your Android phone's notifications from your Windows device or perform other actions related to the notifications. To activate this Phone Link feature, you must enable certain permissions,

such as sync notifications, on both your Windows device and Android phone. These permissions can be revoked at any time under the Phone Link Settings page on your Windows device and your Android phone's settings. For detailed information, see our support page.

Phone Screen Mirroring. On supported devices, Phone Link allows you to view your Android phone's screen on your Windows device. Your Android phone screen will be visible on your Windows device as a pixel stream and any audio that you enable on your Android phone screen while it is linked to your Windows device through Phone Link will play through your Android phone.

Apps mirroring. On supported devices, Phone Link allows you to use your Android apps that are installed on your Android phone on your Windows device. For example, you can launch a music app in your Windows session and listen to audio from that app on your PC speakers. Microsoft collects a list of your installed Android apps and recent activity to provide the service and show you your most

recently used apps. Microsoft does not store what apps you have installed or any of the information displayed by the app in your experience with it.

Content transfer. On supported devices, Phone Link allows you to copy and paste contents such as files, documents, photos, etc. between your Android phone and your Windows device. You can transfer content from your Android phone to your Windows device and from your Windows device to your Android phone by drag and drop contents between the devices.

Instant Hotspot. On supported devices, Link to Windows enables users to share mobile hotspot information with their paired PC over secure Bluetooth communication. Your PC application can then be connected to the internet through the Windows network flyout. Please note mobile data charges may apply depending on the mobile data plan you have.

Contacts sync. Link to Windows allows you to sync your Android contacts into the Microsoft cloud to access them in other Microsoft products and services. You can enable this

feature by going into Link to Windows settings and enabling “Contacts sync” feature. Your contacts information is stored online and associated with your Microsoft account. You may choose to disable sync and delete these contacts at any time. Learn more.

Text-to-voice. Phone Link features include accessibility functionality such as text-to-voice. You can activate a text-to-voice feature, which allows you to hear the contents of a text message or notification as audio. If you activate this feature, your text messages and notifications will be read out loud as they are received.

Office Enterprise. Link to Windows allows you to insert photos into PowerPoint Online and Word Online directly from your mobile phone. This requires your IT Administrator to have enabled Optional Connected Experiences for Microsoft Office applications and you will need to associate your mobile device with your Azure Active Directory (AAD) account and provide Photos permission to your account. After onboarding, your session will last 15

minutes to enable you to transfer your Photos from your mobile device. In order to use this feature again, you will need to scan your QR code again. Link to Windows does not collect your AAD account or information about your Enterprise. In order to provide this service, Microsoft uses a cloud service to relay your files for the purpose of inserting the photos into your PowerPoint Online or Word Online files.

Security and safety features

Device encryption. Device encryption helps protect the data stored on your device by encrypting it using BitLocker Drive Encryption technology. When device encryption is on, Windows automatically encrypts the drive Windows is installed on and generates a recovery key. The BitLocker recovery key for your personal device is automatically backed up online in your personal Microsoft OneDrive account. Microsoft doesn't use your individual recovery keys for any purpose.

Malicious Software Removal Tool. The Malicious Software Removal Tool (MSRT) runs

on your device at least once per month as part of Windows Update. MSRT checks devices for infections by specific, prevalent malicious software ("malware") and helps remove any infections found. When the MSRT runs, it will remove the malware listed on the Microsoft Support website if the malware is on your device. During a malware check, a report will be sent to Microsoft with specific data about malware detected, errors, and other data about your device. If you do not want MSRT to send this data to Microsoft, you can disable MSRT's reporting component.

Microsoft Family. Parents can use Microsoft Family Safety to understand and set boundaries on how their child is using their device. Please carefully review the information at Microsoft Family Safety if choosing to create or join a family group. If you live in a region that requires permission to create an account to access Microsoft services, you may be prompted to request or give parental consent. If a user is under the statutory age in your region, during the registration process they will be prompted to request consent from

a parent or guardian by entering an adult's email. When Family activity reporting is turned on for a child, Microsoft will collect details about how the child uses their device and provide parents with reports of that child's activities. Activity reports are routinely deleted from Microsoft servers.

Microsoft Defender SmartScreen and Smart App Control. Microsoft strives to help protect your device and passwords from unsafe apps, files, and web content.

Microsoft Defender SmartScreen helps protect you when using our services by identifying threats to you, your device, and your passwords. These threats might include potentially unsafe apps or web content that Microsoft Defender SmartScreen discovers while checking websites you visit, files you download, and apps you install and run. When Microsoft Defender SmartScreen checks web and app content, data about the content and your device is sent to Microsoft, including the full web address of the content. When additional analysis is needed to identify

security threats, information about the suspicious website or app—such as content displayed, sounds played, and application memory—may be sent to Microsoft. This data will only be used for security purposes in detecting, protecting against, and responding to security incidents, identity theft, fraud, or other malicious, deceptive, or illegal activities. If Microsoft Defender SmartScreen detects that content is potentially unsafe, you will see a warning in place of the content. Microsoft Defender SmartScreen can be turned on or off in the Windows Security app.

Where supported, Smart App Control helps check software that is installed and runs on your device to determine if it is malicious, potentially unwanted, or poses other threats to you and your device. On a supported device, Smart App Control starts in evaluation mode and the data we collect for Microsoft Defender SmartScreen such as file name, a hash of the file's contents, the download location, and the file's digital certificates, is used to help determine whether your device is a good candidate to use Smart App Control for

additional security protection. Smart App Control is not enabled and will not block during evaluation mode. Some devices may not be good candidates if Smart App Control would otherwise get in the way and interfere with a user's otherwise intended and legitimate tasks – for instance, developers who use a lot of unsigned files. If you are a good candidate for Smart App Control, then it will automatically be turned on, and will provide additional protection to your device beyond Microsoft Defender SmartScreen. Otherwise, Smart App Control will be unavailable and permanently turned off. If your device is unsupported or not a good candidate for Smart App Control, Microsoft Defender SmartScreen will continue to help protect your device. When Smart App Control is enabled and identifies an app as malicious, potentially unwanted, or unknown and unsigned, it will block and notify you prior to opening, running, or installing the app. Learn more about Smart App Control.

When either Microsoft Defender SmartScreen or Smart App Control checks a file, data about that file is sent to Microsoft, including the file

name, a hash of the file's contents, the download location, and the file's digital certificates.

Smart App Control can be turned on or off in the Windows Security app.

Microsoft Defender Antivirus. Microsoft Defender Antivirus looks for malware and other unwanted software, potentially unwanted apps, and other malicious content on your device. Microsoft Defender Antivirus is automatically turned on to help protect your device if no other antimalware software is actively protecting your device. If Microsoft Defender Antivirus is turned on, it will monitor the security status of your device. When Microsoft Defender Antivirus is turned on, or is running because Limited Periodic Scanning is enabled, it will automatically send reports to Microsoft that contain data about suspected malware and other unwanted software, potentially unwanted apps, and other malicious content, and it may also send files that could contain malicious content, such as malware or unknown files for further

inspection. If a report is likely to contain personal data, the report is not sent automatically, and you'll be prompted before it is sent. You can configure Microsoft Defender Antivirus not to send reports and suspected malware to Microsoft.

Speech, Voice Activation, Inking, and Typing

Speech. Microsoft provides both a device-based speech recognition feature and cloud-based (online) speech recognition technologies.

Turning on the Online speech recognition setting lets apps use Microsoft cloud-based speech recognition. Additionally, in Windows 10, the Online speech recognition setting enables your ability to use dictation within Windows.

Turning on speech while setting up a HoloLens device or installing Windows Mixed Reality allows you to use your voice for commands, dictation, and app interactions. Both device-based speech recognition and online speech

recognition settings will be enabled. With both settings enabled, while your headset is turned on the device will always be listening to your voice input and will send your voice data to Microsoft's cloud-based speech recognition technologies.

When you use cloud-based speech recognition technologies from Microsoft, whether enabled by the Online speech recognition setting or when you interact with HoloLens or voice typing, Microsoft collects and uses your voice recordings to provide the speech recognition service by creating a text transcription of the spoken words in the voice data. Microsoft will not store, sample, or listen to your voice recordings without your permission. To learn more about how Microsoft manages your voice data, see Speech recognition technologies.

You can use device-based speech recognition without sending your voice data to Microsoft. However, Microsoft cloud-based speech recognition technologies provide more accurate recognition than the device-based

speech recognition. When the online speech recognition setting is turned off, speech services that do not rely on the cloud and only use device-based recognition—like the live captions app, the Narrator app or the Windows Speech Recognition app—will still work and Microsoft won't collect any voice data.

You can turn off online speech recognition at any time. This will stop any apps that rely on the Online speech recognition setting from sending your voice data to Microsoft. If you are using a HoloLens or Windows Mixed Reality headset, you can also turn off device-based speech recognition at any time. This will stop the device from listening for your voice input. Learn more about speech recognition in Windows.

Voice Activation. Windows provides supported apps with the ability to respond and take action based on voice keywords that are specific to that app—for example allowing Cortana to listen and respond when you say "Cortana."

If you've given permission for an app to listen for voice keywords, Windows will be actively listening to the microphone for these keywords. Once a keyword is recognized, the app will have access to your voice recording, can process the recording, take action, and respond, such as with a spoken answer. The app may send the voice recording to its own services in the cloud to process the commands. Each app should ask you for permission before accessing voice recordings.

Additionally, voice activation can be enabled when the device is locked. If enabled, the relevant app will continue listening to the microphone for voice keywords when you have locked your device and can activate for anyone who speaks near the device. When the device is locked, the app will have access to the same set of capabilities and information as when the device is unlocked.

You can turn off voice activation at any time. Learn more about voice activation in Windows.

Even when you've turned off voice activation, some third-party desktop apps and services

could still be listening to the microphone and collect your voice input. Learn more about third-party desktop apps and how they may still be able to access your microphone even with these settings turned off.

Voice typing. In Windows 11, dictation has been updated and renamed as voice typing. Voice typing may use both device-based and online speech recognition technologies to power its speech-to-text transcription service. You can also choose to contribute voice clips to help improve voice typing. If you choose not to contribute voice clips, you can still use voice typing. You can change your selection anytime in the voice typing settings. Microsoft will not store, sample, or listen to your voice recordings without your permission. Learn more about Microsoft and your voice data.

Voice access. Windows enables everyone, including people with mobility disabilities, to control their PC and author text using their voice. For example, voice access supports scenarios like opening and switching between apps, browsing the web, and reading and

authoring mail. Voice access leverages modern, on-device speech recognition to accurately recognize speech and is supported without an internet connection. Learn more about voice access.

Inking & Typing Personalization. Your typed and handwritten words are collected to provide you with a custom word list, better character recognition to help you type and write on your device, and text suggestions that appear as you type or write.

You can turn off inking & typing personalization at any time. This will delete your customer word list stored on your device. If you turn it back on, you'll need to recreate your custom word list. Learn more about inking & typing personalization in Windows.

Sync and backup settings

When you sign into Windows with your Microsoft account or work or school account, Windows can store your settings, files, and device configuration data in Microsoft's servers. Windows will only use the stored

settings, files, and device configuration data to make it easier for you to migrate your experience on a different device.

You can turn off this feature and stop Windows from storing your settings, files, and configuration data from the Windows settings app. You can also delete the sync and backup data Windows has stored in the settings app.

Learn more about Windows backup and sync settings.

Update Services

Update Services for Windows includes Windows Update and Microsoft Update. Windows Update is a service that provides you with software updates for Windows software and other supporting software, such as drivers and firmware supplied by device manufacturers. Microsoft Update is a service that provides you with software updates for other Microsoft software such as Microsoft 365.

Windows Update automatically downloads Windows software updates to your device. You

can configure Windows Update to automatically install these updates as they become available (recommended) or have Windows notify you when a restart is required to finish installing updates. Apps available through the Microsoft Store are automatically updated through the Microsoft Store, as described in the Microsoft Store section of this privacy statement.

Web browsers—Microsoft Edge Legacy and Internet Explorer

This section applies to legacy versions of Microsoft Edge (versions 44 and below). See the Microsoft Edge section of the Privacy Statement for information about non-legacy versions of Microsoft Edge.

Microsoft Edge is the default web browser for Windows. Internet Explorer, the legacy browser from Microsoft, is also available in Windows. Whenever you use a web browser to access the internet, data about your device ("standard device data") is sent to the websites you visit and online services you use. Standard device data includes your device's IP address,

browser type and language, access times, and referring website addresses. This data might be logged on those websites' web servers. Which data is logged and how that data is used depends on the privacy practices of the websites you visit and web services you use. Additionally, Microsoft Edge sends a unique browser ID to certain websites to enable us to develop aggregate data used to improve browser features and services.

Additionally, data about how you use your browser, such as your browsing history, web form data, temporary internet files, and cookies, is stored on your device. You can delete this data from your device using Delete Browsing History.

Microsoft Edge allows you to capture and save content on your device, such as:

- **Web note**. Allows you to create ink and text annotations on the webpages you visit, and clip, save, or share them.
- **Active reading**. Allows you to create and manage reading lists, including websites or documents.

- **Hub**. Allows you to easily manage your reading lists, favorites, downloads, and history all in one area.
- **Website Pin to Taskbar**. Allows you to pin your favorite websites to the Windows taskbar. Websites will be able to see which of their webpages you have pinned, so they can provide you a notification badge letting you know there is something new for you to check out on their websites.

Some Microsoft browser information saved on your device will be synced across other devices when you sign in with your Microsoft account. For instance, in Internet Explorer, this information includes your browsing history and favorites; and in Microsoft Edge, it includes your favorites, reading lists, autofill form entries (such as your name, address, and phone number), and may include data for extensions that you have installed. As an example, if you sync your Microsoft Edge reading list across devices, copies of the content you choose to save to your reading list will be sent to each synced device for later viewing. You can disable syncing in Internet

Explorer by going to **Start** > **Settings** > **Accounts** > **Sync your settings**. (For more information, see the Sync settings section of this privacy statement.) You can also disable syncing of Microsoft Edge browser information by turning off the sync option in Microsoft Edge Settings.

Microsoft Edge and Internet Explorer use your search queries and browsing history to provide you with faster browsing and more relevant search results. These features include:

- **Search suggestions** in Internet Explorer automatically sends the information you type into the browser address bar to your default search provider (such as Bing) to offer search recommendations as you type each character.
- **Search and site suggestions** in Microsoft Edge automatically sends the information you type into the browser address bar to Bing (even if you have selected another default search provider) to offer search recommendations as you type each character.

You can turn off these features at any time. In order to provide search results, Microsoft Edge and Internet Explorer send your search queries, standard device information, and location (if you have location enabled) to your default search provider. If Bing is your default search provider, we use this data as described in the Bing section of this privacy statement.

Cortana can assist you with your web browsing in Microsoft Edge with features such as Ask Cortana. You can disable Cortana assistance in Microsoft Edge at any time in Microsoft Edge Settings. To learn more about how Cortana uses data and how you can control that, go to the Cortana section of this privacy statement.

Windows apps

A number of Microsoft apps are included with Windows and others are available in Microsoft Store. Some of those apps include:

Maps app. The Maps app provides location-based services and uses Bing services to process your searches within the Maps app.

When the Maps app has access to your location, and you have enabled location-based services in Windows, when you use the “@” key to initiate a search in supported text boxes in Windows apps, Bing services collects the text you type after the “@” key to provide location-based suggestions. To learn more about these Bing-powered experiences, see the Bing section of this privacy statement. When the Maps app has access to your location, even when the app is not in use, Microsoft may collect de-identified location data from your device to improve Microsoft services. You can disable the Maps app's access to your location by turning off the location service or turning off the Maps app's access to the location service.

You can keep track of your favorite places and recent map searches in the Maps app. Your favorite places and search history will be included as search suggestions. If you're signed in with your Microsoft account, your favorite places, search history, and certain app settings will be synced across other devices and services (for example, Cortana). For more

information, see the Sync and backup settings section of this privacy statement.

Camera app. If you allow the Camera app to use your location, location data is embedded in the photos and videos you take with your device. Other descriptive data, such as camera model and the date that the picture or video was taken, is also embedded in photos and videos. If you choose to share a photo or video, any embedded data will be accessible to the people and services you share with. Once enabled, you can always disable the Camera app's access to your location by turning off all access to the location service in your device's Settings menu or turning off the Camera app's access to the location service.

When the Camera app is open, it shows rectangles detected by the selected camera for areas in the image that are potentially used for image enhancement. The Camera app does not retain any image enhancing data. You can always change your camera access settings in the Camera app’s Settings menu or the Windows Settings menu.

Photos app. There are two versions of the Photos app available. The updated Photos app includes features like iCloud integration and local and cloud folder views. The previous legacy version of the Photos app includes features like Video Editor, the People tab, and Albums. You are using the updated Photos app if the “About” section in the Photos app settings indicates the app is the “Updated” Photos app. In some cases, a user may have both the updated Photos app and the Photos legacy version downloaded on their device.

The updated Photos app helps you organize, view, and share your photos and videos. For example, the Photos app presents different ways to group photos and videos by name, date taken, or date modified, and also in folders where those files are stored, such as stored locally on your device or synced to your device from OneDrive, iCloud, and other cloud services. The app also allows you to move, copy or upload files to different locations on your computer or to OneDrive. The All Photos tab displays your locally stored or synced photos and videos according to the date they

are taken. The Favorites tab lets you view photos and videos you previously liked or favorited. The Folders tab allows you to view photos or videos by their storage location. There are also tabs where you can see your photos and videos from available cloud services (such as OneDrive and other third-party services) that you have synced to your device.

The Photos legacy app also helps you organize, view, and share your photos and videos. However, if you are using the Photos legacy app, you may see other features that are not available in the newer version of the Photos app, including Collections, Albums, Video Editor and the People setting. The Collection tab displays photos and videos according to the date they are taken. The Albums tab helps you organize your photos and videos by location and common tags. The Video Editor allows you to edit, create, and share videos.

The People setting can be enabled on the Photos legacy app's Settings page and in the

People tab of the app. When enabled, the Photos legacy app will use face grouping technology to organize your photos and videos into groups. The grouping feature can detect faces in a photo or video and determine whether they are visually similar to faces in other photos and videos in your local photo collection. You can choose to associate a facial grouping with a contact from your People app.

When enabled in the Photos legacy app, your groupings will be stored on your device for as long as you choose to keep the groupings or the photos or videos. If the People setting is turned on, there will be a prompt to allow the Photos legacy app to continue to permit facial groupings after three years of non-interaction with the Photos legacy app. At any time, you can go to the Settings page in the Photos legacy app to turn the People setting on or off. Turning the feature off will remove facial grouping data from the Photos legacy app but will not remove your photos or videos. Learn more about the Photos legacy app and facial grouping.

If you choose to share a photo or video using the Photos app or the Photos legacy app, any embedded data (such as location, camera model, and date) will be accessible to the people and services you share the photo or video with.

People app. The People app lets you see and interact with all your contacts in one place. When you add an account to the People app, your contacts from your account will be automatically added to the People app. You can add other accounts to the People app, including your social networks (such as Facebook and Twitter) and email accounts. When you add an account, we tell you what data the People app can import or sync with the particular service and let you choose what you want to add. Other apps you install may also sync data to the People app, including providing additional details to existing contacts. When you view a contact in the People app, information about your recent interactions with the contact (such as emails and calendar events, including from apps that the People app syncs data from) will be

retrieved and displayed to you. You can remove an account from the People app at any time.

Mail and Calendar app. The Mail and Calendar app allows you to connect all your email, calendars, and files in one place, including those from third-party email and file storage providers. The app provides location-based services, such as weather information in your calendar, but you can disable the app's use of your location. When you add an account to the Mail and Calendar app, your email, calendar items, files, contacts, and other settings from your account will automatically sync to your device and to Microsoft servers. At any time, you can remove an account or make changes to the data that's synced from your account. To configure an account, you must provide the app with the account credentials (such as user name and password), which will be sent over the internet to the third-party provider's server. The app will first attempt to use a secure (SSL) connection to configure your account but will send this information unencrypted if your email provider does not support SSL. If you

add an account provided by an organization (such as a company email address), the owner of the organizational domain can implement certain policies and controls (for example, multi-factor authentication or the ability to remotely wipe data from your device) that may affect your use of the app.

Messaging app. When you sign in with a Microsoft account on your device, you can choose to back up your information, which will sync your SMS and MMS messages and store them in your Microsoft account. This allows you to retrieve the messages if you lose or change phones. After your initial device set-up, you can manage your messaging settings at any time. Turning off your SMS/MMS backup will not delete messages that have been previously backed up to your Microsoft account. To delete such messages, you must first delete them from your device prior to turning off backup. If you allow the Messaging app to use your location, you can attach a link to your current location to an outgoing message. Location information will be collected by Microsoft as described in the

Windows Location services section of this privacy statement.

Narrator. Narrator is a screen-reading app that helps you use Windows without a screen. Narrator offers intelligent image and page title description and web page summaries when you encounter undescribed images and ambiguous links.

When you choose to get an image description by pressing Narrator + Ctrl + D, the image will be sent to Microsoft to perform analysis of the image and generate a description. Images are used only to generate the description and are not stored by Microsoft.

When you choose to get page title descriptions by pressing Narrator + Ctrl + D, the URL of the site you are visiting will be sent to Microsoft to generate the page title description and to provide and improve Microsoft services, such as Bing services as described in the Bing section above.

When you choose to get a list of popular links for a web page by pressing Narrator + double press of S, the URL of the site you are visiting

will be sent to Microsoft to generate the summary of popular links and to provide and improve Microsoft services, such as Bing.

You can disable these features at any time by going to **Narrator > Get image descriptions, page titles and popular links** in the Windows setting app.

You can also send feedback about Narrator to help Microsoft diagnose and resolve problems with Narrator and improve Microsoft products and services, such as Windows. Verbal feedback can be submitted at any time in Narrator by using Narrator Key + Alt + F. When you use this command, the Feedback Hub app will launch, giving you the opportunity to submit verbal feedback. If you enable the setting “Help Make Narrator Better” in the Windows settings app and submit verbal feedback through Feedback Hub, recent device and usage data, including event trace log (ETL) data, will be submitted along with your verbal feedback to improve Microsoft products and services, such as Windows.

Live captions. Live captions transcribe audio to help with the comprehension of spoken content. Live captions can generate captions from any audio containing speech, whether the audio is online, audio you have downloaded to your device, or audio received from your microphone. By default, transcribing microphone audio is disabled.

Voice data that is captioned is only processed on your device and is not shared to the cloud or with Microsoft. Learn more about live captions.

Windows Media Player

Windows Media Player allows you to play CDs, DVDs, and other digital content (such as WMA and MP3 files), rip CDs, and manage your media library. To enrich your experience when you play content in your library, Windows Media player displays related media information, such as album title, song titles, album art, artist, and composer. To augment your media information, Windows Media player will send a request to Microsoft which contains standard computer information, an

identifier for the media content, and the media information already contained in your Windows Media Player library (including information you may have edited or entered yourself) so that Microsoft can recognize the track and then return additional information that is available.

Windows Media Player also allows you to play back content that is streamed to you over a network. To provide this service, it is necessary for Windows Media Player to communicate with a streaming media server. These servers are typically operated by non-Microsoft content providers. During playback of streaming media, Windows Media Player will send a log to the streaming media server or other web server(s) if the streaming media server requests it. The log includes such details as: connection time, IP address, operating system version, Windows Media Player version, Player identification number (Player ID), date, and protocol. To protect your privacy, Windows Media Player defaults to sending a Player ID that is different for each session.

Windows Hello

Windows Hello provides instant access to your devices through biometric authentication. If you turn it on, Windows Hello uses your face, fingerprint, or iris to identify you based on a set of unique points or features that are extracted from the image and stored on your device as a template—but it does not store the actual image of your face, fingerprint, or iris. Biometric verification data that's used when you sign in doesn't leave your device. Your biometric verification data will remain on your device until you remove it. However, after a significant period of Windows Hello inactivity, you will be prompted to confirm that you want to continue to store your biometric verification data. You can delete your biometric verification data from within Settings. Learn more about Windows Hello.

Windows Search

Windows Search lets you search your stuff and the web from one place. If you choose to use Windows Search to search "your stuff," it will

provide results for items on your personal OneDrive, your OneDrive for Business if so enabled, other cloud storage providers to the extent supported by those third-party providers, and on your device. If you choose to use Windows Search to search the web, or get search suggestions with Windows Search, your search results will be powered by Bing and we will use your search query as described in the Bing section of this privacy statement. Learn more about search in Windows.

Entertainment and related services

Entertainment and Related Services power rich experiences and enable you to access a variety of content, applications and games.

Xbox

The Xbox network is the online gaming and entertainment service from Microsoft that consists of software and enables online experiences across different platforms. This service lets you find and play games, view content, and connect with friends on Xbox and

other gaming and social networks. You can connect to the Xbox network using Xbox consoles, Windows devices, and mobile devices (Android and iPhone).

When you sign up for an Xbox profile, we assign you a gamertag (a public nickname) and a unique identifier. When you sign in on Xbox devices, apps, and services, the data we collect about your use is stored using these unique identifier(s).

Xbox consoles are devices you can use to find and play games, movies, music, and other digital entertainment. When you sign in to Xbox experiences—in apps or on a console—we also assign a unique identifier to your device. When your Xbox console is connected to the internet, for instance, and you sign in to the console, we identify which console and which version of the console's operating system you're using.

Xbox continues to provide new experiences in client apps that are connected to and backed by services such as the Xbox network and cloud gaming. When signed in to an Xbox

experience, we collect required data to help keep these experiences reliable, up to date, secure, and performing as expected.

Data we collect about your use of Xbox services, games, apps, and consoles includes:

- When you sign in and sign out of Xbox, any purchases you make, and content you obtain.
- Which games you play and apps you use, your game progress, achievements, play time per game, and other play statistics.
- Performance data about Xbox consoles, Xbox Game Pass and other Xbox apps, the Xbox network, connected accessories, and your network connection, including any software or hardware errors.
- Content you add, upload, or share through the Xbox network, including text, pictures, and video you capture in games and apps.
- Social activity, including chat data and interactions with other gamers, and connections you make (friends you add and people who follow you) on the Xbox network.

If you use an Xbox console or Xbox app on another device capable of accessing the Xbox network, and that device includes a storage device (hard drive or memory unit), usage data will be stored on the storage device and sent to Microsoft the next time you sign in to Xbox, even if you've been playing offline.

Xbox console diagnostic data. Diagnostic data has two categories: required and optional. If you use an Xbox console, the console will send required data to Microsoft. Optional data is additional data that you choose to share with Microsoft.

- **Required**. The minimum data necessary to help keep Xbox safe, secure, up to date, and performing as expected.
- **Optional**. Optional data includes additional details about your console, its settings, its health, its use, and enhanced error reporting to help us detect, diagnose, and fix problems.

Learn more at Manage settings for optional data sharing.

Game captures. Any player in a multiplayer game session can record video (game clips) and capture screenshots of their view of the game play. Other players' game clips and screenshots can capture your in-game character and gamertag during that session. If a player captures game clips and screenshots on a PC, the resulting game clips might also capture audio chat.

Captioning. During Xbox real-time ("party") chat, players may activate a voice-to-text feature that lets them view that chat as text. If a player activates this feature, all voice communication in the party is captioned for the player. Microsoft uses the resulting text data to provide captioning of chat for players who need it, as well as the other purposes described in this statement.

Data use. Microsoft uses the data we collect to improve gaming products and experiences—making them safer and more fun over time.

Data we collect also enables us to provide you with personalized, curated experiences. This includes connecting you to games, content,

and services, as well as presenting you with offers, discounts, and recommendations.

Xbox data viewable by others. Your gamertag, game and play statistics, achievements, presence (whether you are currently signed in to Xbox), content you share, and other data about your activity on Xbox can be seen by:

- Other players signed in to Xbox.
- Customers of third-party services you've linked your profile to, or
- Other services associated with Xbox (including those of partner companies).

For example, your gamertag and scores that show on game leaderboards are considered public and cannot be hidden. For other data, you can adjust your privacy settings on consoles and at Xbox.com to limit or block what is shared with the public or with friends.

Learn more at Xbox online safety and privacy settings.

Xbox data shared with third parties including game and apps publishers. When you use an Xbox online game or any network-connected

app on your Xbox console, PC, or mobile device, the publisher of that game or app has access to data about your usage to help the publisher deliver, support, and improve its product. This data may include: your Xbox user identifier, gamertag, limited account info such as country and age range, data about your in-game communications, any Xbox enforcement activity, game-play sessions (for example, moves made in-game, types of vehicles used in-game), your presence on the Xbox network, the time you spend playing the game or app, rankings, statistics, gamer profiles, avatars, or gamerpics, friends lists, activity feeds for official clubs you belong to, official club memberships, and any content you create or submit in the game or app.

Third-party publishers and developers of games and apps have their own distinct and independent relationship with users and their collection and usage of personal data is subject to their specific privacy policies. You should carefully review their policies to determine how they use the data. For example, publishers may choose to disclose or display

game data (such as on leaderboards) through their own services. You may find their policies linked from game or app detail pages in the Microsoft Store.

Learn more at Data Sharing with Games and Apps.

To stop sharing game or app data with a publisher, remove its games or app from all devices where you have installed them. Some publisher access to your data may be revoked at https://microsoft.com/consent.

Children and family. If you have kids who want to use the Xbox network, you can set up child and teen profiles for them once they have Microsoft accounts. Adult organizers in your Microsoft family group can change consent choices and online safety settings for child and teen profiles on Xbox.com.

Learn more about Microsoft family groups at Simplify your family's life.

Learn more about managing Xbox profiles, at Xbox online safety and privacy settings.

For more information about Microsoft's collection of data from children, including Xbox, please see the Collection of data from children section of this privacy statement.

Safety. In order to help make the Xbox network a safe gaming environment and enforce the Community Standards for Xbox, we may collect and review voice, text, images, videos and in-game content (such as game clips you upload, conversations you have, and things you post in clubs and games).

Anti-cheat and fraud prevention. Providing a fair gameplay environment is important to us. We prohibit cheating, hacking, account stealing, and any other unauthorized or fraudulent activity when you use an Xbox online game or any network-connected app on your Xbox console, PC, or mobile device. In order to detect and prevent fraud and cheating, we may use anti-cheat and fraud prevention tools, applications, and other technologies. Such technologies may create digital signatures (known as "hashes") using certain information collected from your Xbox console,

PC, or mobile device, and how you use that device. This can include information about the browser, device, activities, game identifiers, and operating system.

Legacy.

- **Xbox 360**. This Xbox console collects limited required diagnostic data to keep your console functioning as expected while using a console connected to the Xbox network.
- **Kinect**. The Kinect sensor is a combination of camera, microphone, and infrared sensor that can enable motions and voice to be used to control gameplay. For example:
  - If you choose, the camera can be used to sign you in to the Xbox network automatically using facial recognition. This data stays on the console and is not shared with anyone, and you can choose to delete this data from your console at any time.
  - For game play, Kinect will map distances between your body's joints to create a

stick figure representation of you that helps Kinect enable play.
    - The Kinect microphone can enable voice chat between players during play. The microphone also enables voice commands for control of the console, game, or app, or to enter search terms.
    - The Kinect sensor can also be used for audio and video communications through services such as Skype.

Learn more about Kinect at Xbox Kinect and Privacy.

Microsoft Store

Microsoft Store is an online service, accessible via PC, the Xbox Console and the Xbox App, that allows you to browse, download, purchase, rate, and review applications and other digital content. It includes:

- Apps and content for Windows devices such as phones, PCs, and tablets.
- Games, subscriptions and other apps for Xbox consoles and other devices.

- Products and apps for Microsoft 365, SharePoint, Exchange, Access, and Project (2013 versions or later).

We collect data about how you access and use Microsoft Store; the products you've viewed, purchased, or installed; the preferences you set for viewing apps in Microsoft Store; and any ratings, reviews, or problem reports you submit. Your Microsoft account is associated with your ratings and reviews; and if you write a review, the name and picture from your Microsoft account will be published with your review.

Permission for Microsoft Store apps. Many apps you install from the Microsoft Store are designed to take advantage of specific hardware and software features of your device. An app's use of certain hardware and software features may give the app or its related service access to your data. For example, a photo editing app might access your device's camera to let you take a new photo or access photos or videos stored on your device for editing, and a restaurant guide

might use your location to provide nearby recommendations. Information about the features that an app uses is provided on the app's product description page in Microsoft Store. Many of the features that Microsoft Store apps use can be turned on or off through your device's privacy settings. In Windows, in many cases, you can choose which apps can use a particular feature. Go to **Start > Settings > Privacy or Privacy & Security**, select the feature (for example, Calendar), and then select which app permissions are on or off. The lists of apps in Windows privacy settings that can use hardware and software features will not include "Classic Windows" applications, and these applications are not affected by these settings.

App updates. Unless you have turned off automatic app updates in the relevant Microsoft Store settings or have acquired an app provided and updated by the app developer, Microsoft Store will automatically check for, download, and install app updates to verify that you have the latest versions. Updated apps might use different Windows

hardware and software features from the previous versions, which could give them access to different data on your device. You will be prompted for consent if an updated app accesses certain features, such as location. You can also review the hardware and software features an app uses by viewing its product description page in Microsoft Store.

Each app's use of your data collected through any of these features is subject to the app developer's privacy policies. If an app available through Microsoft Store collects and uses any of your personal data, the app developer is required to provide a privacy policy, and a link to the privacy policy is available on the app's product description page in Microsoft Store.

Sideloaded apps and developer mode. Developer features such as the "developer mode" setting are intended for development use only. If you enable developer features, your device may become unreliable or unusable, and expose you to security risks. Downloading or otherwise acquiring apps from sources other than Microsoft Store, also known as

"sideloading" apps, may make your device and personal data more vulnerable to attack or unexpected use by apps. Windows policies, notifications, permissions, and other features intended to help protect your privacy when apps access your data may not function as described in this statement for sideloaded apps or when developer features are enabled.

Microsoft Start

Microsoft Start is a content service that includes news, weather, sports, and finance. The Microsoft Start app is available on various platforms, including iOS and Android. The Microsoft Start service is also included within other Microsoft services, including the Microsoft Edge browser and widgets on Windows.

When you install the Microsoft Start app, we collect data that tells us if the app was installed properly, the installation date, the app version, and other data about your device such as the operating system and browser. This data is collected on a regular basis to help us determine the number of Microsoft Start app

users and identify performance issues associated with different app versions, operating systems, and browsers.

We also collect data about how you interact with Microsoft Start content, such as usage frequency and articles viewed, to provide you with relevant content. Microsoft Start provides an enhanced experience when you sign in with your Microsoft account, including allowing you to customize your interests and favorites. You can manage personalization through Microsoft Start and Bing settings, as well as through settings in other Microsoft services that include Microsoft Start services. We also use the data we collect to provide you with advertisements that may be of interest to you. You can opt out of interest-based advertising through the advertising links within Microsoft Start services, or by visiting the Microsoft opt-out page.

Previous versions of MSN Money allow you to access personal finance information from third-party financial institutions. MSN Money only displays this information and does not

store it on our servers. Your sign-in credentials used to access your financial information from third parties are encrypted on your device and are not sent to Microsoft. These financial institutions, as well as any other third-party services you access through MSN services, are subject to their own terms and privacy policies.

Groove Music and Movies & TV

Groove Music lets you easily play your music collection and make playlists. Microsoft Movies & TV allows you to play your video collection and rent or buy movies and TV episodes. These services were formerly offered as Xbox Music and Video.

To help you discover content that may interest you, Microsoft will collect data about what content you play, the length of play, and the rating you give it.

To enrich your experience when playing content, Groove Music and Movies & TV will display related information about the content you play and the content in your music and

video libraries, such as the album title, cover art, song or video title, and other information, where available. To provide this information, Groove Music and Movies & TV send an information request to Microsoft containing standard device data, such as your device IP address, device software version, your regional and language settings, and an identifier for the content.

If you use Movies & TV to access content that has been protected with Microsoft Digital Rights Management (DRM), it may automatically request media usage rights from an online rights server and download and install DRM updates in order to let you play the content. See the DRM information in the Silverlight section of this privacy statement for more information.

Silverlight

Microsoft Silverlight helps you to access and enjoy rich content on the Web. Silverlight enables websites and services to store data on your device. Other Silverlight features involve connecting to Microsoft to obtain updates, or

to Microsoft or third-party servers to play protected digital content.

Silverlight Configuration tool. You can make choices about these features in the Silverlight Configuration tool. To access the Silverlight Configuration tool, right click on content that is currently being displayed by Silverlight and select **Silverlight**. You can also run the Silverlight Configuration tool directly. In Windows, for example, you can access the tool by searching for "Microsoft Silverlight."

Silverlight application storage. Silverlight-based applications can store data files locally on your computer for a variety of purposes, including saving your custom settings, storing large files for graphically intensive features (such as games, maps, and images), and storing content that you create within certain applications. You can turn off or configure application storage in the Silverlight Configuration tool.

Silverlight updates. Silverlight will periodically check a Microsoft server for updates to provide you with the latest features and

improvements. A small file containing information about the latest Silverlight version will be downloaded to your computer and compared to your currently installed version. If a newer version is available, it will be downloaded and installed on your computer. You can turn off or configure updates in the Silverlight Configuration tool.

Digital Rights Management. Silverlight uses Microsoft Digital Rights Management (DRM) technology to help protect the rights of content owners. If you access DRM-protected content (such as music or video) with Silverlight, it will request media usage rights from a rights server on the Internet. In order to provide a seamless playback experience, you will not be prompted before Silverlight sends the request to the rights server. When requesting media usage rights, Silverlight will provide the rights server with an ID for the DRM-protected content file and basic data about your device, including data about the DRM components on your device such as their revision and security levels, and a unique identifier for your device.

DRM updates. In some cases, accessing DRM-protected content will require an update to Silverlight or to the DRM components on your device. When you attempt to play content that requires a DRM update, Silverlight will send a request to a Microsoft server containing basic data about your device, including information about the DRM components on your computer such as their revision and security levels, troubleshooting data, and a unique identifier for your device. The Microsoft server uses this identifier to return a unique DRM update for your device, which will then be installed by Silverlight. You can turn off or configure DRM component updates on the **Playback** tab in the Silverlight Configuration tool.

Windows Mixed Reality

Windows Mixed Reality allows you to enable a virtual reality experience that immerses you in apps and games. Mixed Reality uses a compatible headset’s camera, microphone, and infrared sensors to enable motions and voice to be used to control gameplay and to navigate apps and games.

Microsoft collects diagnostic data to solve problems and to keep Mixed Reality running on Windows up to date, secure, and operating properly. Diagnostic data also helps us improve Mixed Reality and related Microsoft products and services depending on the diagnostic data settings you've chosen for your device. Learn more about Windows diagnostic data.

Mixed Reality also processes and collects data specifically related to the Mixed Reality experiences, such as:

- Mixed Reality maps distances between your body's joints to create a stick figure representation of you. If you are connected to the Internet, we collect those numeric values to enable and improve your experience.
- Mixed Reality detects specific hand gestures intended to perform simple system interactions (such as menu navigation, pan/zoom, and scroll). This data is processed on your PC and is not stored.

- The headset's microphones enable voice commands to control games, apps, or to enter search terms. Learn more about voice data collection.
- Windows Mixed Reality can also be used for audio and video communications through services such as Skype.

Personal data we collect

Microsoft collects data from you, through our interactions with you and through our products for a variety of purposes described below, including to operate effectively and provide you with the best experiences with our products. You provide some of this data directly, such as when you create a Microsoft account, administer your organization's licensing account, submit a search query to Bing, register for a Microsoft event, speak a voice command to Cortana, upload a document to OneDrive, sign up for Microsoft 365, or contact us for support. We get some of it by collecting data about your interactions, use, and experience with our products and communications.

We rely on a variety of legal reasons and permissions (sometimes called "legal bases") to

process data, including with your consent, a balancing of legitimate interests, necessity to enter into and perform contracts, and compliance with legal obligations, for a variety of purposes described below.

We also obtain data from third parties. We protect data obtained from third parties according to the practices described in this statement, plus any additional restrictions imposed by the source of the data. These third-party sources vary over time and include:

- Data brokers from which we purchase demographic data to supplement the data we collect.
- Services that make user-generated content from their service available to others, such as local business reviews or public social media posts.
- Communication services, including email providers and social networks, when you give us permission to access your data on such third-party services or networks.
- Service providers that help us determine your device’s location.

- Partners with which we offer co-branded services or engage in joint marketing activities.
- Developers who create experiences through or for Microsoft products.
- Third parties that deliver experiences through Microsoft products.
- Publicly-available sources, such as open public sector, academic, and commercial data sets and other data sources.

If you represent an organization, such as a business or school, that utilizes Enterprise and Developer Products from Microsoft, please see the Enterprise and developer products section of this privacy statement to learn how we process your data. If you are an end user of a Microsoft product or a Microsoft account provided by your organization, please see the Products provided by your organization and the Microsoft account sections for more information.

You have choices when it comes to the technology you use and the data you share. When you are asked to provide personal data, you can decline. Many of our products require some personal data to operate and provide you with a service. If you

choose not to provide data required to operate and provide you with a product or feature, you cannot use that product or feature. Likewise, where we need to collect personal data by law or to enter into or carry out a contract with you, and you do not provide the data, we will not be able to enter into the contract; or if this relates to an existing product you're using, we may have to suspend or cancel it. We will notify you if this is the case at the time. Where providing the data is optional, and you choose not to share personal data, features like personalization that use the data will not work for you.

The data we collect depends on the context of your interactions with Microsoft and the choices you make (including your privacy settings), the products and features you use, your location, and applicable law.

The data we collect can include the following:

Name and contact data. Your first and last name, email address, postal address, phone number, and other similar contact data.

Credentials. Passwords, password hints, and similar security information used for

authentication and account access.

Demographic data. Data about you such as your age, gender, country, and preferred language.

Payment data. Data to process payments, such as your payment instrument number (such as a credit card number) and the security code associated with your payment instrument.

Subscription and licensing data. Information about your subscriptions, licenses, and other entitlements.

Interactions. Data about your use of Microsoft products. In some cases, such as search queries, this is data you provide in order to make use of the products. In other cases, such as error reports, this is data we generate. Other examples of interactions data include:

- **Device and usage data**. Data about your device and the product and features you use, including information about your hardware and software, how our products perform, as well as your settings. For example:
  - **Payment and account history**. Data about the items you purchase and activities

associated with your account.

- **Browse history**. Data about the webpages you visit.
- **Device, connectivity, and configuration data**. Data about your device, your device configuration, and nearby networks. For example, data about the operating systems and other software installed on your device, including product keys. In addition, IP address, device identifiers (such as the IMEI number for phones), regional and language settings, and information about WLAN access points near your device.
- **Error reports and performance data**. Data about the performance of the products and any problems you experience, including error reports. Error reports (sometimes called “crash dumps”) can include details of the software or hardware related to an error, contents of files opened when an error occurred, and data about other software on your device.
- **Troubleshooting and help data**. Data you provide when you contact Microsoft for help, such as the products you use, and other

details that help us provide support. For example, contact or authentication data, the content of your chats and other communications with Microsoft, data about the condition of your device, and the products you use related to your help inquiry. When you contact us, such as for customer support, phone conversations or chat sessions with our representatives may be monitored and recorded.
    - **Bot usage data**. Interactions with bots and skills available through Microsoft products, including bots and skills provided by third parties.
- **Interests and favorites**. Data about your interests and favorites, such as the sports teams you follow, the programming languages you prefer, the stocks you track, or cities you add to track things like weather or traffic. In addition to those you explicitly provide, your interests and favorites can also be inferred or derived from other data we collect.
- **Content consumption data**. Information about media content (e.g., TV, video, music, audio, text

books, apps, and games) you access through our products.

- **Searches and commands**. Search queries and commands when you use Microsoft products with search or related productivity functionality, such as interactions with a chat bot.
- **Voice data**. Your voice data, sometimes referred to as “voice clips”, such as search queries, commands, or dictation you speak, which may include background sounds.
- **Text, inking, and typing data**. Text, inking, and typing data and related information. For example, when we collect inking data, we collect information about the placement of your inking instrument on your device.
- **Images**. Images and related information, such as picture metadata. For example, we collect the image you provide when you use a Bing image-enabled service.
- **Contacts and relationships**. Data about your contacts and relationships if you use a product to share information with others, manage contacts, communicate with others, or improve your productivity.

- **Social data**. Information about your relationships and interactions between you, other people, and organizations, such as types of engagement (e.g., likes, dislikes, events, etc.) related to people and organizations.
- **Location data**. Data about your device's location, which can be either precise or imprecise. For example, we collect location data using Global Navigation Satellite System (GNSS) (e.g., GPS) and data about nearby cell towers and Wi-Fi hotspots. Location can also be inferred from a device's IP address or data in your account profile that indicates where it is located with less precision, such as at a city or postal code level.
- **Other input**. Other inputs provided when you use our products. For example, data such as the buttons you press on an Xbox wireless controller using the Xbox network, skeletal tracking data when you use Kinect, and other sensor data, like the number of steps you take, when you use devices that have applicable sensors. And, if you use Spend, at your direction, we also collect financial transaction data from your credit card issuer to provide the

service. If you attend an in-store event, we collect the data you provide to us when registering for or during the event and if you enter into a prize promotion, we collect the data you input into the entry form.

Content. Content of your files and communications you input, upload, receive, create, and control. For example, if you transmit a file using Skype to another Skype user, we need to collect the content of that file to display it to you and the other user. If you receive an email using Outlook.com, we need to collect the content of that email to deliver it to your inbox, display it to you, enable you to reply to it, and store it for you until you choose to delete it. Other content we collect when providing products to you include:

- Communications, including audio, video, text (typed, inked, dictated, or otherwise), in a message, email, call, meeting request, or chat.
- Photos, images, songs, movies, software, and other media or documents you store, retrieve, or otherwise process with our cloud.

Video or recordings. Recordings of events and activities at Microsoft buildings, retail spaces, and

other locations. If you enter Microsoft Store locations or other facilities, or attend a Microsoft event that is recorded, we may process your image and voice data.

Feedback and ratings. Information you provide to us and the content of messages you send to us, such as feedback, survey data, and product reviews you write.

Traffic data. Data generated through your use of Microsoft's communications services. Traffic data indicates with whom you have communicated and when your communications occurred. We will process your traffic data only as required to provide, maintain, and improve our communications services and we do so with your consent.

Product-specific sections below describe data collection practices applicable to use of those products.

How we use personal data

Microsoft uses the data we collect to provide you rich, interactive experiences. In particular, we use data to:

- Provide our products, which includes updating, securing, and troubleshooting, as well as providing support. It also includes sharing data, when it is required to provide the service or carry out the transactions you request.
- Improve and develop our products.
- Personalize our products and make recommendations.
- Advertise and market to you, which includes sending promotional communications, targeting advertising, and presenting you relevant offers.

We also use the data to operate our business, which includes analyzing our performance, meeting our legal obligations, developing our workforce, and doing research.

For these purposes, we combine data we collect from different contexts (for example, from your use of two Microsoft products). For example, Cortana may use information from your calendar to suggest action items in a heads-up email, and Microsoft Store uses information about the apps and services you use to make personalized app recommendations. However, we have built in technological and procedural safeguards designed

to prevent certain data combinations where required by law. For example, where required by law, we store data we collect from you when you are unauthenticated (not signed in) separately from any account information that directly identifies you, such as your name, email address, or phone number.

Our processing of personal data for these purposes includes both automated and manual (human) methods of processing. Our automated methods often are related to and supported by our manual methods. For example, to build, train, and improve the accuracy of our automated methods of processing (including artificial intelligence or AI), we manually review some of the predictions and inferences produced by the automated methods against the underlying data from which the predictions and inferences were made. For instance, with your permission and for the purpose of improving our speech recognition technologies, we manually review short snippets of voice data that we have taken steps to de-identify. This manual review may be conducted by Microsoft employees or vendors who are working on Microsoft's behalf.

When we process personal data about you, we do so with your consent and/or as required to provide the products you use, operate our business, meet our contractual and legal obligations, protect the security of our systems and our customers, or fulfill other legitimate interests of Microsoft as described in this section and in the Reasons we share personal data section of this privacy statement. When we transfer personal data from the European Economic Area, we do so based on a variety of legal mechanisms, as described in the Where we store and process personal data section of this privacy statement.

More on the purposes of processing:

- **Provide our products**. We use data to operate our products and provide you with rich, interactive experiences. For example, if you use OneDrive, we process the documents you upload to OneDrive to enable you to retrieve, delete, edit, forward, or otherwise process it, at your direction as part of the service. Or, for example, if you enter a search query in the Bing search engine, we use that query to display search results to you. Additionally, as

communications are a feature of various products, programs, and activities, we use data to contact you. For example, we may contact you by phone or email or other means to inform you when a subscription is ending or discuss your licensing account. We also communicate with you to secure our products, for example by letting you know when product updates are available.

- **Product improvement**. We use data to continually improve our products, including adding new features or capabilities. For example, we use error reports to improve security features, search queries and clicks in Bing to improve the relevancy of the search results, usage data to determine what new features to prioritize, and voice data to develop and improve speech recognition accuracy.
- **Personalization**. Many products include personalized features, such as recommendations that enhance your productivity and enjoyment. These features use automated processes to tailor your product experiences based on the data we have about you, such as inferences we make about you and

your use of the product, activities, interests, and location. For example, depending on your settings, if you stream movies in a browser on your Windows device, you may see a recommendation for an app from the Microsoft Store that streams more efficiently. If you have a Microsoft account, with your permission, we can sync your settings on several devices. Many of our products provide controls to disable personalized features.

- **Product activation**. We use data—such as device and application type, location, and unique device, application, network, and subscription identifiers—to activate products that require activation.
- **Product development**. We use data to develop new products. For example, we use data, often de-identified, to better understand our customers' computing and productivity needs which can shape the development of new products.
- **Customer support**. We use data to troubleshoot and diagnose product problems, repair customers' devices, and provide other customer care and support services, including to help us

provide, improve, and secure the quality of our products, services, and training, and to investigate security incidents. Call recording data may also be used to authenticate or identify you based on your voice to enable Microsoft to provide support services and investigate security incidents.

- **Help secure and troubleshoot**. We use data to help secure and troubleshoot our products. This includes using data to protect the security and safety of our products and customers, detecting malware and malicious activities, troubleshooting performance and compatibility issues to help customers get the most out of their experiences, and notifying customers of updates to our products. This may include using automated systems to detect security and safety issues.
- **Safety**. We use data to protect the safety of our products and our customers. Our security features and products can disrupt the operation of malicious software and notify users if malicious software is found on their devices. For example, some of our products, such as Outlook.com or OneDrive, systematically scan

content in an automated manner to identify suspected spam, viruses, abusive actions, or URLs that have been flagged as fraud, phishing, or malware links; and we reserve the right to block delivery of a communication or remove content if it violates our terms. **In accordance with European Union Regulation (EU) 2021/1232, we have invoked the derogation permitted by that Regulation from Articles 5(1) and 6(1) of EU Directive 2002/58/EC. We use scanning technologies to create digital signatures (known as "hashes") of certain images and video content on our systems. These technologies then compare the hashes they generate with hashes of reported child sexual exploitation and abuse imagery (known as a "hash set"), in a process called "hash matching". Microsoft obtains hash sets from organizations that act in the public interest against child sex abuse. This can result in sharing information with the National Center for Missing and Exploited Children (NCMEC) and law enforcement authorities.**

- **Updates**. We use data we collect to develop product updates and security patches. For

example, we may use information about your device's capabilities, such as available memory, to provide you a software update or security patch. Updates and patches are intended to maximize your experience with our products, help you protect the privacy and security of your data, provide new features, and evaluate whether your device is ready to process such updates.

- **Promotional communications**. We use data we collect to deliver promotional communications. You can sign up for email subscriptions and choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail, and telephone. For information about managing your contact data, email subscriptions, and promotional communications, see the How to access and control your personal data section of this privacy statement.
- **Relevant offers**. Microsoft uses data to provide you with relevant and valuable information regarding our products. We analyze data from a variety of sources to predict the information that will be most interesting and relevant to you

and deliver such information to you in a variety of ways. For example, we may predict your interest in gaming and communicate with you about new games you may like.

- **Advertising**. Microsoft does not use what you say in email, human-to-human chat, video calls, or voice mail, or your documents, photos, or other personal files to target ads to you. We use data we collect through our interactions with you, through some of our first-party products, services, apps, and web properties (Microsoft properties), and on third-party web properties, for advertising on our Microsoft properties and on third-party properties. We may use automated processes to help make advertising more relevant to you. For more information about how your data is used for advertising, see the Advertising section of this privacy statement.
- **Prize promotions and events**. We use your data to administer prize promotions and events available in our physical Microsoft Stores. For example, if you enter into a prize promotion, we may use your data to select a winner and provide the prize to you if you win. Or, if you

register for a coding workshop or gaming event, we will add your name to the list of expected attendees.

- **Transacting commerce**. We use data to carry out your transactions with us. For example, we process payment information to provide customers with product subscriptions and use contact information to deliver goods purchased from the Microsoft Store.
- **Reporting and business operations**. We use data to analyze our operations and perform business intelligence. This enables us to make informed decisions and report on the performance of our business.
- **Protecting rights and property**. We use data to detect and prevent fraud, resolve disputes, enforce agreements, and protect our property. For example, we use data to confirm the validity of software licenses to reduce piracy. We may use automated processes to detect and prevent activities that violate our rights and the rights of others, such as fraud.
- **Legal compliance**. We process data to comply with law. For example, we use the age of our customers to assist us in meeting our

obligations to protect children's privacy. We also process contact information and credentials to help customers exercise their data protection rights.
- **Research.** With appropriate technical and organizational measures to safeguard individuals' rights and freedoms, we use data to conduct research, including for public interest and scientific purposes.

Reasons we share personal data

We share your personal data with your consent or as necessary to complete any transaction or provide any product you have requested or authorized. For example, we share your content with third parties when you tell us to do so, such as when you send an email to a friend, share photos and documents on OneDrive, or link accounts with another service. If you use a Microsoft product provided by an organization you are affiliated with, such as an employer or school, or use an email address provided by such organization to access Microsoft products, we share certain data, such as interaction data and diagnostic data to enable your organization to manage the products. When you

provide payment data to make a purchase, we will share payment data with banks and other entities that process payment transactions or provide other financial services, and for fraud prevention and credit risk reduction. Additionally, when you save a payment method (such as a card) to your account that you and other Microsoft account holders use to make purchases from Microsoft or its affiliates, your purchase receipts may be shared with anyone else who uses and has access to the same payment method to make a purchase from Microsoft, including the payment method's named accountholder. When you permit push notifications for Microsoft products or applications on a non-Windows device, the operating system of that device will process some personal data to provide push notifications. Accordingly, Microsoft may send data to an external, third-party notification provider to deliver push notifications. Your device's push notification services are governed by their own service-specific terms and privacy statements.

In addition, we share personal data among Microsoft-controlled affiliates and subsidiaries. We also share personal data with vendors or agents

working on our behalf for the purposes described in this statement. For example, companies we've hired to provide customer service support or assist in protecting and securing our systems and services may need access to personal data to provide those functions. In such cases, these companies must abide by our data privacy and security requirements and are not allowed to use personal data they receive from us for any other purpose. We may also disclose personal data as part of a corporate transaction such as a merger or sale of assets.

Finally, we will retain, access, transfer, disclose, and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to do any of the following:

- Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies.
- Protect our customers, for example, to prevent spam or attempts to defraud users of our

products, or to help prevent the loss of life or serious injury of anyone.
- Operate and maintain the security of our products, including to prevent or stop an attack on our computer systems or networks.
- Protect the rights or property of Microsoft, including enforcing the terms governing the use of the services—however, if we receive information indicating that someone is using our services to traffic in stolen intellectual or physical property of Microsoft, we will not inspect a customer's private content ourselves, but we may refer the matter to law enforcement.

For more information about data we disclose in response to requests from law enforcement and other government agencies, please see our Law Enforcement Requests Report.

Please note that some of our products include links to or otherwise enable you to access products of third parties whose privacy practices differ from those of Microsoft. If you provide personal data to any of those products, your data is governed by their privacy policies.

How to access and control your personal data

You can also make choices about the collection and use of your data by Microsoft. You can control your personal data that Microsoft has obtained, and exercise your data protection rights, by contacting Microsoft or using various tools we provide. In some cases, your ability to access or control your personal data will be limited, as required or permitted by applicable law. How you can access or control your personal data will also depend on which products you use. For example, you can:

- Control the use of your data for personalized advertising from Microsoft by visiting our opt-out page.
- Choose whether you wish to receive promotional emails, SMS messages, telephone calls, and postal mail from Microsoft.
- Access and clear some of your data through the Microsoft privacy dashboard.

Not all personal data processed by Microsoft can be accessed or controlled via the tools above. If

you want to access or control personal data processed by Microsoft that is not available via the tools above or directly through the Microsoft products you use, you can always contact Microsoft at the address in the How to contact us section or by using our web form.

We provide aggregate metrics about user requests to exercise their data protection rights via the Microsoft Privacy Report.

You can access and control your personal data that Microsoft has obtained with tools Microsoft provides to you, which are described below, or by contacting Microsoft. For instance:

- If Microsoft obtained your consent to use your personal data, you can withdraw that consent at any time.
- You can request access to, erasure of, and updates to your personal data.
- If you'd like to port your data elsewhere, you can use tools Microsoft provides to do so, or if none are available, you can contact Microsoft for assistance.

You can also object to or restrict the use of your personal data by Microsoft. For example, you can

object at any time to our use of your personal data:

- For direct marketing purposes.
- Where we are performing a task in the public interest or pursuing our legitimate interests or those of a third party.

You may have these rights under applicable laws, including the EU General Data Protection Regulation (GDPR), but we offer them regardless of your location. In some cases, your ability to access or control your personal data will be limited, as required or permitted by applicable law.

If your organization, such as your employer, school, or service provider, provides you with access to and is administering your use of Microsoft products, contact your organization to learn more about how to access and control your personal data.

You can access and control your personal data that Microsoft has obtained, and exercise your data protection rights, using various tools we provide. The tools most useful to you will depend on our interactions with you and your use of our products. Here is a general list of tools we provide

to help you control your personal data; specific products may provide additional controls.

- **Bing.** If you are signed into Bing, you can view and clear your stored search and chat history on your privacy dashboard. If you are not signed into Bing, you can view and clear stored search history associated to your device in your Bing settings.
- **Cortana.** You can control some of the data Cortana accesses or stores in your Cortana settings.
- **Microsoft account.** If you wish to access, edit, or remove the profile information and payment information in your Microsoft account, change your password, add security information or close your account, you can do so by visiting the Microsoft account website.
- If you have a **Microsoft Developer Network** (MSDN) public profile, you can access and edit your data by signing in at MSDN forum.
- **Microsoft privacy dashboard**. You can control some of the data Microsoft processes through your use of a Microsoft account on the Microsoft privacy dashboard. From here, for example, you can view and clear the browsing,

search, and location data associated with your Microsoft account.

- **Microsoft Store.** You can access your Microsoft Store profile and account information by visiting Microsoft Store and selecting **View account** or **Order history.**
- **Microsoft Teams for personal use.** You can find out how to export or delete Teams data relating to your personal Microsoft account by visiting this page.
- **OneDrive.** You can view, download, and delete your files and photos in OneDrive by signing into your OneDrive.
- **Outlook.com.** You can download your emails in Outlook.com by signing into your account and navigating to your **Privacy and data** settings.
- **Skype**. If you wish to access, edit, or remove some profile and payment information for Skype or change your password, sign in to your account. If you wish to export your Skype chat history and files shared on Skype, you can request a copy.
- **Volume Licensing Service Center (VLSC).** If you are a Volume Licensing customer, you can control your contact information and

subscription and licensing data in one location by visiting the Volume Licensing Service Center website.

- **Xbox**. If you use the Xbox network or Xbox.com, you can view or edit your personal data, including billing and account information, privacy settings, and online safety and data sharing preferences by accessing My Xbox on the Xbox console or on the Xbox.com website.

Not all personal data processed by Microsoft can be accessed or controlled via the tools above. If you want to access or control personal data processed by Microsoft that is not available via the tools above or directly through the Microsoft products you use, you can always contact Microsoft at the address in the How to contact us section or by using our web form. We will respond to requests to control your personal data as required by applicable law.

Your communications preferences

You can choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail, and telephone. If you receive promotional email or SMS messages from

us and would like to opt out, you can do so by following the directions in that message. You can also make choices about the receipt of promotional email, telephone calls, and postal mail by signing in with your personal Microsoft account, and viewing your communication permissions where you can update contact information, manage Microsoft-wide contact preferences, opt out of email subscriptions, and choose whether to share your contact information with Microsoft partners. If you do not have a personal Microsoft account, you can manage your Microsoft email contact preferences by using this web form. These choices do not apply to mandatory service communications that are part of certain Microsoft products, programs, activities, or to surveys or other informational communications that have their own unsubscribe method.

Your advertising choices

To opt out of receiving personalized advertising from Microsoft, visit our opt-out page. When you opt out, your preference is stored in a cookie that is specific to the web browser you are using. The opt-out cookie has an expiration date of five years.

If you delete the cookies on your device, you need to opt out again.

You can also link your opt-out choice with your personal Microsoft account. It will then apply on any device where you use that account and will continue to apply until someone signs in with a different personal Microsoft account on that device. If you delete the cookies on your device, you will need to sign in again for the settings to apply.

For Microsoft-controlled advertising that appears in apps on Windows, you may use the opt-out linked to your personal Microsoft account, or opt out of interest-based advertising by turning off the advertising ID in Windows settings.

Because the data used for interest-based advertising is also used for other required purposes (including providing our products, analytics, and fraud detection), opting out of interest-based advertising does not stop that data collection. You will continue to get ads, although they may be less relevant to you.

You can opt out of receiving interest-based advertising from third parties we partner with by

visiting their sites (see above).

Browser-based controls

When you use a browser, you can control your personal data using certain features. For example:

- **Cookie controls**. You can control the data stored by cookies and withdraw consent to cookies by using the browser-based cookie controls described in the Cookies section of this privacy statement.
- **Tracking protections**. You can control the data third-party sites can collect about you using Tracking Protection in Internet Explorer (versions 9 and up) and Microsoft Edge. This feature will block third-party content, including cookies, from any site that is listed in a Tracking Protection List you add.
- **Browser controls for "Do Not Track."** Some browsers have incorporated "Do Not Track" (DNT) features that can send a signal to the websites you visit indicating you do not wish to be tracked. Because there is not yet a common understanding of how to interpret the DNT signal, Microsoft services do not currently respond to browser DNT signals. We continue to

work with the online industry to define a common understanding of how to treat DNT signals. In the meantime, you can use the range of other tools we provide to control data collection and use, including the ability to opt out of receiving interest-based advertising from Microsoft as described above.

Cookies and similar technologies

Cookies are small text files placed on your device to store data that can be recalled by a web server in the domain that placed the cookie. This data often consists of a string of numbers and letters that uniquely identifies your computer, but it can contain other information as well. Some cookies are placed by third parties acting on our behalf. We use cookies and similar technologies to store and honor your preferences and settings, enable you to sign-in, provide interest-based advertising, combat fraud, analyze how our products perform, and fulfill other legitimate purposes described below. Microsoft apps use additional identifiers, such as the advertising ID in Windows, for similar purposes, and many of our websites and

applications also contain web beacons or other similar technologies, as described below.

Our use of cookies and similar technologies

Microsoft uses cookies and similar technologies for several purposes, depending on the context or product, including:

- **Storing your preferences and settings**. We use cookies to store your preferences and settings on your device, and to enhance your experiences. For example, depending on your settings, if you enter your city or postal code to get local news or weather information on a Microsoft website, we store that data in a cookie so that you will see the relevant local information when you return to the site. Saving your preferences with cookies, such as your preferred language, prevents you from having to set your preferences repeatedly. If you opt out of interest-based advertising, we store your opt-out preference in a cookie on your device. Similarly, in scenarios where we obtain your consent to place cookies on your device, we store your choice in a cookie.

- **Sign-in and authentication**. We use cookies to authenticate you. When you sign in to a website using your personal Microsoft account, we store a unique ID number, and the time you signed in, in an encrypted cookie on your device. This cookie allows you to move from page to page within the site without having to sign in again on each page. You can also save your sign-in information so you do not have to sign in each time you return to the site.
- **Security**. We use cookies to process information that helps us secure our products, as well as detect fraud and abuse.
- **Storing information you provide to a website**. We use cookies to remember information you shared. When you provide information to Microsoft, such as when you add products to a shopping cart on Microsoft websites, we store the data in a cookie for the purpose of remembering the information.
- **Social media**. Some of our websites include social media cookies, including those that enable users who are signed in to the social media service to share content via that service.

- **Feedback**. Microsoft uses cookies to enable you to provide feedback on a website.
- **Interest-based advertising**. Microsoft uses cookies to collect data about your online activity and identify your interests so that we can provide advertising that is most relevant to you. You can opt out of receiving interest-based advertising from Microsoft as described in the How to access and control your personal data section of this privacy statement.
- **Showing advertising**. Microsoft uses cookies to record how many visitors have clicked on an advertisement and to record which advertisements you have seen, for example, so you do not see the same one repeatedly.
- **Analytics**. We use first- and third-party cookies and other identifiers to gather usage and performance data. For example, we use cookies to count the number of unique visitors to a web page or service and to develop other statistics about the operations of our products.
- **Performance**. Microsoft uses cookies to understand and improve how our products perform. For example, we use cookies to gather

data that helps with load balancing; this helps us keep our websites remain up and running.

Where required, we obtain your consent prior to placing or using optional cookies that are not (i) strictly necessary to provide the website; or (ii) for the purpose of facilitating a communication. Please see the “How to Control Cookies” section below for more information.

Some of the cookies we commonly use are listed below. This list is not exhaustive, but it is intended to illustrate the primary purposes for which we typically set cookies. If you visit one of our websites, the site will set some or all of the following cookies:

- **MSCC**. Contains user choices for most Microsoft properties.
- **MUID, MC1, and MSFPC**. Identifies unique web browsers visiting Microsoft sites. These cookies are used for advertising, site analytics, and other operational purposes.
- **ANON**. Contains the ANID, a unique identifier derived from your Microsoft account, which is used for advertising, personalization, and operational purposes. It is also used to preserve

your choice to opt out of interest-based advertising from Microsoft if you have chosen to associate the opt-out with your Microsoft account.

- **CC**. Contains a country code as determined from your IP address.
- **PPAuth, MSPAuth, MSNRPSAuth, KievRPSAuth, WLSSC, MSPProf**. Helps to authenticate you when you sign in with your Microsoft account.
- **MC0**. Detects whether cookies are enabled in the browser.
- **MS0**. Identifies a specific session.
- **NAP**. Contains an encrypted version of your country, postal code, age, gender, language and occupation, if known, based on your Microsoft account profile.
- **MH**. Appears on co-branded sites where Microsoft is partnering with an advertiser. This cookie identifies the advertiser, so the right ad is selected.
- **childinfo, kcdob, kcrelid, kcru, pcfm**. Contains information that Microsoft account uses within its pages in relation to child accounts.

- **MR**. This cookie is used by Microsoft to reset or refresh the MUID cookie.
- **x-ms-gateway-slice**. Identifies a gateway for load balancing.
- **TOptOut**. Records your decision not to receive interest-based advertising delivered by Microsoft. Where required, we place this cookie by default and remove it when you consent to interest-based advertising.

We may also use the cookies of other Microsoft affiliates, companies, and partners, such as LinkedIn and Xandr.

Third Party Cookies

In addition to the cookies Microsoft sets when you visit our websites, we also use cookies from third parties to enhance the services on our sites. Some third parties can also set cookies when you visit Microsoft sites. For example:

- Companies we hire to provide services on our behalf, such as site analytics, place cookies when you visit our sites.
- Companies that deliver content on Microsoft sites, such as videos or news, or ads, place cookies on their own.

These companies use the data they process in accordance with their privacy policies, which may enable these companies to collect and combine information about your activities across websites, apps, or online services.

The following types of third-party cookies may be used, depending on the context, service or product, as well as your settings and permissions:

- **Social Media cookies.** We and third parties use social media cookies to show you ads and content based on your social media profiles and activity on our websites. They're used to connect your activity on our websites to your social media profiles so the ads and content you see on our websites and on social media will better reflect your interests.
- **Analytics cookies.**We allow third parties to use analytics cookies to understand how you use our websites so we can make them better and the third parties can develop and improve their products, which they may use on websites that are not owned or operated by Microsoft. For example, analytics cookies are used to gather information about the pages you visit and how

many clicks you need to accomplish a task. These cookies may also be used for advertising purposes.

- **Advertising cookies.**We and third parties use advertising cookies to show you new ads by recording which ads you've already seen. They're also used to track which ads you click on or purchases you make after clicking on an ad for payment purposes, and to show you ads that are more relevant to you. For example, they're used to detect when you click on an ad and show you ads based on your social media interests and website browsing history.
- **Required cookies.**We use required cookies to perform essential website functions. For example, to log you in, save your language preferences, provide a shopping cart experience, improve performance, route traffic between web servers, detect the size of your screen, determine page load times, and measure audiences. These cookies are necessary for our websites to work.

Where required, we obtain your consent prior to placing or using optional cookies that are not (i)

strictly necessary to provide the website; or (ii) for the purpose of facilitating a communication.

For a list of the third parties that set cookies on our websites, including service providers acting on our behalf, please visit our third party cookie inventory. The third party cookie inventory also includes links to those third parties' websites or privacy notices. Please consult the third party websites or privacy notices for more information on their privacy practices with respect to their cookies that may be set on our websites. On some of our websites, a list of third parties is available directly on the site. The third parties on these sites may not be included in the list on our third party cookie inventory.

How to control cookies

Most web browsers automatically accept cookies but provide controls that allow you to block or delete them. For example, in Microsoft Edge, you can block or delete cookies by selecting **Settings** > **Privacy and services** > **Clear Browsing data** > **Cookies and other site data**. For more information about how to delete your cookies in Microsoft browsers, see Microsoft Edge, Microsoft Edge

Legacy, or Internet Explorer. If you use a different browser, refer to that browser's instructions.

As mentioned above, where required, we obtain your consent before placing or using optional cookies that are not (i) strictly necessary to provide the website; or (ii) for the purpose of facilitating a communication. We separate these optional cookies by purpose, such as for advertising and social media purposes. You may consent to certain categories of optional cookies and not others. You also may adjust your choices by clicking "Manage cookies" in the footer of the website or through the settings made available on the website. Certain features of Microsoft products depend on cookies. If you choose to block cookies, you cannot sign in or use some of those features, and preferences that are dependent on cookies will be lost. If you choose to delete cookies, any settings and preferences controlled by those cookies, including advertising preferences, are deleted and will need to be recreated.

Additional privacy controls that can impact cookies, including the tracking protections feature

of Microsoft browsers, are described in the How to access and control your personal data section of this privacy statement.

Our use of web beacons and analytics services

Some Microsoft webpages contain electronic tags known as web beacons that we use to help deliver cookies on our websites, count users who have visited those websites, and deliver co-branded products. We also include web beacons or similar technologies in our electronic communications to determine whether you open and act on them.

In addition to placing web beacons on our own websites, we sometimes work with other companies to place our web beacons on their websites or in their advertisements. This helps us to, for example, develop statistics on how often clicking on an advertisement on a Microsoft website results in a purchase or other action on the advertiser's website. It also allows us to understand your activity on the website of a Microsoft partner in connection with your use of a Microsoft product or service.

Finally, Microsoft products often contain web beacons or similar technologies from third-party

analytics providers, which help us compile aggregated statistics about the effectiveness of our promotional campaigns or other operations. These technologies enable the analytics providers to set or read their own cookies or other identifiers on your device, through which they can collect information about your online activities across applications, websites, or other products. However, we prohibit these analytics providers from using web beacons on our sites to collect or access information that directly identifies you (such as your name or email address). You can opt out of data collection or use by some of these analytics providers by visiting any of the following sites: Adjust, AppsFlyer, Clicktale, Flurry Analytics, Google Analytics (requires you to install a browser add-on), Kissmetrics, Mixpanel, Nielsen, Acuity Ads, WebTrends, or Optimizely.

Other similar technologies

In addition to standard cookies and web beacons, our products can also use other similar technologies to store and read data files on your computer. This is typically done to maintain your preferences or to improve speed and performance

by storing certain files locally. But, like standard cookies, these technologies can also store a unique identifier for your computer, which can then track behavior. These technologies include Local Shared Objects (or "Flash cookies") and Silverlight Application Storage.

Local Shared Objects or "Flash cookies." Websites that use Adobe Flash technologies can use Local Shared Objects or "Flash cookies" to store data on your computer. To learn how to manage or block Flash cookies, go to the Flash Player help page.

Silverlight Application Storage. Websites or applications that use Microsoft Silverlight technology also have the ability to store data by using Silverlight Application Storage. To learn how to manage or block such storage, see the Silverlight section of this privacy statement.

Products provided by your organization—notice to end users

If you use a Microsoft product with an account provided by an organization you are affiliated with, such as your work or school account, that organization can:

- Control and administer your Microsoft product and product account, including controlling privacy-related settings of the product or product account.
- Access and process your data, including the interaction data, diagnostic data, and the contents of your communications and files associated with your Microsoft product and product accounts.

If you lose access to your work or school account (in event of change of employment, for example), you may lose access to products and the content associated with those products, including those you acquired on your own behalf, if you used your work or school account to sign in to such products.

Many Microsoft products are intended for use by organizations, such as schools and businesses. Please see the Enterprise and developer products section of this privacy statement. If your organization provides you with access to Microsoft products, your use of the Microsoft products is subject to your organization's policies, if any. You should direct your privacy inquiries, including any

requests to exercise your data protection rights, to your organization's administrator. When you use social features in Microsoft products, other users in your network may see some of your activity. To learn more about the social features and other functionality, please review documentation or help content specific to the Microsoft product. Microsoft is not responsible for the privacy or security practices of our customers, which may differ from those set forth in this privacy statement.

When you use a Microsoft product provided by your organization, Microsoft's processing of your personal data in connection with that product is governed by a contract between Microsoft and your organization. Microsoft processes your personal data to provide the product to your organization and you, and in some cases for Microsoft's business operations related to providing the product as described in the Enterprise and developer products section. As mentioned above, if you have questions about Microsoft's processing of your personal data in connection with providing products to your organization, please contact your organization. If

you have questions about Microsoft's business operations in connection with providing products to your organization as provided in the Product Terms, please contact Microsoft as described in the How to contact us section. For more information on our business operations, please see the Enterprise and developer products section.

For Microsoft products provided by your K-12 school, including Microsoft 365 Education, Microsoft will:

- not collect or use student personal data beyond that needed for authorized educational or school purposes;
- not sell or rent student personal data;
- not use or share student personal data for advertising or similar commercial purposes, such as behavioral targeting of advertisements to students;
- not build a personal profile of a student, other than for supporting authorized educational or school purposes or as authorized by the parent, guardian, or student of appropriate age; and
- require that our vendors with whom student personal data is shared to deliver the

educational service, if any, are obligated to implement these same commitments for student personal data.

Microsoft account

With a Microsoft account, you can sign into Microsoft products, as well as those of select Microsoft partners. Personal data associated with your Microsoft account includes credentials, name and contact data, payment data, device and usage data, your contacts, information about your activities, and your interests and favorites. Signing into your Microsoft account enables personalization, consistent experiences across products and devices, permits you to use cloud data storage, allows you to make payments using payment instruments stored in your Microsoft account, and enables other features. There are three types of Microsoft account:

- When you create your own Microsoft account tied to your personal email address, we refer to that account as a **personal Microsoft account**.
- When you or your organization (such as an employer or your school) create your Microsoft account tied to your email address provided by

that organization, we refer to that account as a **work or school account**.
- When you or your service provider (such as a cable or internet service provider) create your Microsoft account tied to your email address with your service provider's domain, we refer to that account as a **third-party account**.

Personal Microsoft accounts. The data associated with your personal Microsoft account, and how that data is used, depends on how you use the account.

- **Creating your Microsoft account**. When you create a personal Microsoft account, you will be asked to provide certain personal data and we will assign a unique ID number to identify your account and associated information. While some products, such as those involving payment, require a real name, you can sign in to and use other Microsoft products without providing your real name. Some data you provide, such as your display name, email address, and phone number, can be used to help others find and connect with you within Microsoft products. For example, people who

know your display name, email address, or phone number can use it to search for you on Skype or Microsoft Teams for personal use and send you an invite to connect with them. Note that if you use a work or school email address to create a personal Microsoft account, your employer or school may gain access to your data. In some cases, you will need to change the email address to a personal email address in order to continue accessing consumer-oriented products (such as the Xbox network).

- **Signing in to Microsoft account**. When you sign in to your Microsoft account, we create a record of your sign-in, which includes the date and time, information about the product you signed in to, your sign-in name, the unique number assigned to your account, a unique identifier assigned to your device, your IP address, and your operating system and browser version.
- **Signing in to Microsoft products**. Signing in to your account enables improved personalization, provides seamless and consistent experiences across products and devices, permits you to access and use cloud data storage, allows you to make payments using payment instruments

stored in your Microsoft account, and enables other enhanced features and settings. For example, when you sign in, Microsoft makes information saved to your account available across Microsoft products so important things are right where you need them. When you sign in to your account, you will stay signed in until you sign out. If you add your Microsoft account to a Windows device (version 8 or higher), Windows will automatically sign you in to products that use Microsoft account when you access those products on that device. When you are signed in, some products will display your name or username and your profile photo (if you have added one to your profile) as part of your use of Microsoft products, including in your communications, social interactions, and public posts. Learn more about your Microsoft account, your data, and your choices.

- **Signing in to third-party products**. If you sign in to a third-party product with your Microsoft account, you will share data with the third party in accordance with the third party's privacy policy. The third party will also receive the version number assigned to your account (a

new version number is assigned each time you change your sign-in data); and information that describes whether your account has been deactivated. If you share your profile data, the third party can display your name or user name and your profile photo (if you have added one to your profile) when you are signed in to that third-party product. If you chose to make payments to third-party merchants using your Microsoft account, Microsoft will pass information stored in your Microsoft account to the third party or its vendors (e.g., payment processors) as necessary to process your payment and fulfill your order (such as name, credit card number, billing and shipping addresses, and relevant contact information). The third party can use or share the data it receives when you sign in or make a purchase according to its own practices and policies. **You should carefully review the privacy statement for each product you sign in to and each merchant you purchase from to determine how it will use the data it collects**.

Work or school accounts. The data associated with a work or school account, and how it will be used, is generally similar to the use and collection

of data associated with a personal Microsoft account.

If your employer or school uses Azure Active Directory (AAD) to manage the account it provides you, you can use your work or school account to sign in to Microsoft products, such as Microsoft 365 and Office 365, and third-party products provided to you by your organization. If required by your organization, you will also be asked to provide a phone number or an alternative email address for additional security verification. And, if allowed by your organization, you may also use your work or school account to sign in to Microsoft or third-party products that you acquire for yourself.

If you sign in to Microsoft products with a work or school account, note:

- The owner of the domain associated with your email address may control and administer your account, and access and process your data, including the contents of your communications and files, including data stored in products provided to you by your organization, and products you acquire by yourself.

- Your use of the products is subject to your organization's policies, if any. You should consider both your organization's policies and whether you are comfortable enabling your organization to access your data before you choose to use your work or school account to sign in to products you acquire for yourself.
- If you lose access to your work or school account (if you change employers, for example), you may lose access to products, including content associated with those products, you acquired on your own behalf if you used your work or school account to sign in to such products.
- Microsoft is not responsible for the privacy or security practices of your organization, which may differ from those of Microsoft.
- If your organization is administering your use of Microsoft products, please direct your privacy inquiries, including any requests to exercise your data subject rights, to your administrator. See also the Notice to end users section of this privacy statement.
- If you are uncertain whether your account is a work or school account, please contact your

organization.

Third-party accounts. The data associated with a third-party Microsoft account, and how it will be used, is generally similar to the use and collection of data associated with a personal Microsoft account. Your service provider has control over your account, including the ability to access or delete your account. **You should carefully review the terms the third party provided you to understand what it can do with your account**.

Collection of data from children

For users under the age of 13 or as specified by law in their jurisdiction, certain Microsoft products and services will either block users under that age or will ask them to obtain consent or authorization from a parent or guardian before they can use it, including when creating an account to access Microsoft services. We will not knowingly ask children under that age to provide more data than is required to provide for the product.

Once parental consent or authorization is granted, the child's account is treated much like any other account. The child can access communication

services, like Outlook and Skype, and can freely communicate and share data with other users of all ages. Learn more about parental consent and Microsoft child accounts.

Parents or guardians can change or revoke the consent choices previously made. As the organizer of a Microsoft family group, the parent or guardian can manage a child's information and settings on their Family Safety page and view and delete a child's data on their privacy dashboard. See below for more information about how to access and delete child data.

Below is additional information about the collection of data from children, including more details as related to Xbox.

Accessing and deleting child data. For Microsoft products and services that require parental consent, a parent can view and delete certain data belonging to their child from the parent's privacy dashboard: browsing history, search history, location activity, media activity, apps and service activity, and product and service performance data. To delete this data, a parent can sign in to their privacy dashboard and manage their child's

activities. Please note that a parent's ability to access and/or delete a child's personal information on their privacy dashboard will vary depending on the laws where you are located.

Additionally, a parent can contact our privacy support team through the privacy support form and, following authentication, request that the data types on the privacy dashboard together with the following data be deleted: software, setup, and inventory; device connectivity and configuration; feedback and ratings; fitness and activity; support content; support interactions; and environmental sensor. We process authenticated deletion requests within 30 days of receipt.

Please note that content like emails, contacts, and chats are accessible through in-product experiences. You can find more information about data you are able to control within Microsoft products by visiting our Privacy Frequently Asked Questions (FAQs).

If your child's account is not a part of your Microsoft family group and you do not have access to your child's activity on your privacy dashboard, then you need to submit a request

related to your child's data through the privacy support form. The privacy team will ask for account verification before fulfilling the request.

To delete all of your child's personal information, you must request deletion of the child's account through the close your account form. This link will prompt you to sign in with your child's account credentials. Check that the page shows the correct Microsoft account, and then follow the instructions to request that your child's account be deleted. Learn more about how to close a Microsoft account.

After you submit the request to close your child's account, we will wait 60 days before permanently deleting the account in case you change your mind or need to access something on the account before it is permanently closed and deleted. During the waiting period, the account is marked for closure and permanent deletion, but it still exists. If you want to reopen your child's Microsoft account, just sign in again within that 60-day period. We will cancel the account closure, and the account will be reinstated.

What is Xbox? Xbox is the gaming and entertainment division of Microsoft. Xbox hosts an online network that consists of software and enables online experiences crossing multiple platforms. This network lets your child find and play games, view content, and connect with friends on Xbox and other gaming and social networks. Children can connect to the Xbox network using Xbox consoles, Windows devices, and mobile devices (Android and iPhone).

Xbox consoles are devices your child can use to find and play games, movies, music, and other digital entertainment. When they sign in to Xbox, in apps, games or on a console, we assign a unique identifier to their device. For instance, when their Xbox console is connected to the internet and they sign in to the console, we identify which console and which version of the console's operating system they are using.

Xbox continues to provide new experiences in client apps that are connected to and backed by services such as Xbox network and cloud gaming. When signed in to an Xbox experience, we collect required data to help keep these experiences

reliable, up to date, secure, and performing as expected.

Data we collect when you create an Xbox profile. You as the parent or guardian are required to consent to the collection of personal data from a child under 13 years old or as otherwise specified by your jurisdiction. With your permission, your child can have an Xbox profile and use the online Xbox network. During the child Xbox profile creation, you will sign in with your own Microsoft account to verify that you are an adult organizer in your Microsoft family group. We collect an alternate email address or phone number to boost account security. If your child needs help accessing their account, they will be able to use one of these alternates to validate they own the Microsoft account.

We collect limited information about children, including name, birthdate, email address, and region. When you sign your child up for an Xbox profile, they get a gamertag (a public nickname) and a unique identifier. When you create your child's Xbox profile you consent to Microsoft collecting, using, and

sharing information based on their privacy and communication settings on the Xbox online network. Your child's privacy and communication settings are defaulted to the most restrictive.

Data we collect. We collect information about your child's use of Xbox services, games, apps, and devices including:

- When they sign in and sign out of Xbox, purchase history, and content they obtain.
- Which games they play and apps they use, their game progress, achievements, play time per game, and other play statistics.
- Performance data about Xbox consoles, Xbox Game Pass and other Xbox apps, the Xbox network, connected accessories, and network connection, including any software or hardware errors.
- Content they add, upload, or share through the Xbox network, including text, pictures, and video they capture in games and apps.
- Social activity, including chat data and interactions with other gamers, and connections they make (friends they add and people who follow them) on the Xbox network.

If your child uses an Xbox console or Xbox app on another device capable of accessing the Xbox network, and that device includes a storage device (hard drive or memory unit), usage data will be stored on the storage device and sent to Microsoft the next time they sign in to Xbox, even if they have been playing offline.

Xbox console diagnostic data. If your child uses an Xbox console, the console will send required data to Microsoft. Required data is the minimum data necessary to help keep Xbox safe, secure, up to date, and performing as expected.

Game captures. Any player in a multiplayer game session can record video (game clips) and capture screenshots of their view of the game play. Other players' game clips and screenshots can capture your child's in-game character and gamertag during that session. If a player captures game clips and screenshots on a PC, the resulting game clips might also capture audio chat if your child's privacy and communication settings on the Xbox online network allow it.

Captioning. During Xbox real-time ("party") chat, players may activate a voice-to-text feature that

lets them view that chat as text. If a player activates this feature, Microsoft uses the resulting text data to provide captioning of chat for players who need it. This data may also be used to provide a safe gaming environment and enforce the Community Standards for Xbox.

Data use. Microsoft uses the data we collect to improve gaming products and experiences—making it safer and more fun over time. Data we collect also enables us to provide your child with personalized, curated experiences. This includes connecting them to games, content, services, and recommendations.

Xbox data viewable by others. When your child is using the Xbox network, their online presence (which can be set to "appear offline" or "blocked"), gamertag, game play statistics, and achievements are visible to other players on the network. Depending on how you set your child's Xbox safety settings, they might share information when playing or communicating with others on the Xbox network.

Safety. In order to help make the Xbox network a safe gaming environment and enforce the

Community Standards for Xbox, we may collect and review voice, text, images, videos and in-game content (such as game clips your child uploads, conversations they have, and things they post in clubs and games).

Anti-cheat and fraud prevention. Providing a fair gameplay environment is important to us. We prohibit cheating, hacking, account stealing, and any other unauthorized or fraudulent activity when your child uses an Xbox online game or any network-connected app on their Xbox console, PC, or mobile device. In order to detect and prevent fraud and cheating, we may use anti-cheat and fraud prevention tools, applications, and other technologies. Such technologies may create digital signatures (known as “hashes”) using certain information collected from their Xbox console, PC, or mobile device, and how they use that device. This can include information about the browser, device, activities, game identifiers, and operating system.

Xbox data shared with game and apps publishers. When your child uses an Xbox online game or any network-connected app on their Xbox console, PC,

or mobile device, the publisher of that game or app has access to data about their usage to help the publisher deliver, support, and improve its product. This data may include: your child's Xbox user identifier, gamertag, limited account info such as country and age range, data about your child's in-game communications, any Xbox enforcement activity, game-play sessions (for example, moves made in-game or types of vehicles used in-game), your child's presence on the Xbox network, the time they spend playing the game or app, rankings, statistics, gamer profiles, avatars, or gamerpics, friends lists, activity feeds for official clubs they belong to, official club memberships, and any content they create or submit in the game or app.

Third-party publishers and developers of games and apps have their own distinct and independent relationship with users and their collection and usage of personal data is subject to their specific privacy policies. You should carefully review their policies to determine how they use your child's data. For example, publishers may choose to disclose or display game data (such as on leaderboards) through their own services. You may

find their policies linked from the game or app detail pages in our stores.

Learn more at Data Sharing with Games and Apps.

To stop sharing game or app data with a publisher, remove its games or app from all devices where they have been installed. Some publisher access to your child's data may be revoked at microsoft.com/consent.

Managing child settings. As the organizer of a Microsoft family group, you can manage a child's information and settings on their Family Safety page, as well as their Xbox profile privacy settings from their Xbox Privacy & online safety page.

You can also use the Xbox Family Settings app to manage your child's experience on the Xbox Network including: spending for Microsoft and Xbox stores, viewing your child's Xbox activity, and setting age ratings and the amount of screen time.

Learn more about managing Xbox profiles at Xbox online safety and privacy settings.
Learn more about Microsoft family groups at Simplify your family's life.

Legacy.

- **Xbox 360**. This Xbox console collects limited required diagnostic data. This data helps keep your child's console functioning as expected.
- **Kinect**. The Kinect sensor is a combination of camera, microphone, and infrared sensor that can enable motions and voice to be used to control game play. For example:
  - If you choose, the camera can be used to sign in to the Xbox network automatically using facial recognition. This data stays on the console, is not shared with anyone, and can be deleted at any time.
  - For game play, Kinect will map distances between the joints on your child's body to create a stick figure representation to enable play.
  - The Kinect microphone can enable voice chat between players during play. The microphone also enables voice commands for control of the console, game, or app, or to enter search terms.
  - The Kinect sensor can also be used for audio and video communications through services such as Skype.

Learn more about Kinect at Xbox Kinect and Privacy.

Other important privacy information

Below you will find additional privacy information, such as how we secure your data, where we process your data, and how long we retain your data. You can find more information on Microsoft and our commitment to protecting your privacy at Microsoft Privacy.

Security of personal data

Microsoft is committed to protecting the security of your personal data. We use a variety of security technologies and procedures to help protect your personal data from unauthorized access, use, or disclosure. For example, we store the personal data you provide on computer systems that have limited access and are in controlled facilities. When we transmit highly confidential data (such as a credit card number or password) over the internet, we protect it through the use of encryption. Microsoft complies with applicable

data protection laws, including applicable security breach notification laws.

Where we store and process personal data

Personal data collected by Microsoft may be stored and processed in your region, in the United States, and in any other country where Microsoft or its affiliates, subsidiaries, or service providers operate facilities. Microsoft maintains major data centers in Australia, Austria, Brazil, Canada, Finland, France, Germany, Hong Kong, India, Ireland, Japan, Korea, Luxembourg, Malaysia, the Netherlands, Singapore, South Africa, the United Kingdom, and the United States. Typically, the primary storage location is in the customer's region or in the United States, often with a backup to a data center in another region. The storage location(s) are chosen in order to operate efficiently, to improve performance, and to create redundancies in order to protect the data in the event of an outage or other problem. We take steps to process the data that we collect under this privacy statement

according to this statement's provisions and the requirements of applicable law.

We transfer personal data from the European Economic Area, the United Kingdom, and Switzerland to other countries, some of which have not yet been determined by the European Commission to have an adequate level of data protection. For example, their laws may not guarantee you the same rights, or there may not be a privacy supervisory authority there that is capable of addressing your complaints. When we engage in such transfers, we use a variety of legal mechanisms, including contracts such as the standard contractual clauses published by the European Commission under Commission Implementing Decision 2021/914, to help protect your rights and enable these protections to travel with your data. To learn more about the European Commission's decisions on the adequacy of the protection of personal data in the countries where Microsoft processes personal data, see this article on the European Commission website.

Microsoft Corporation complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Microsoft Corporation has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Microsoft Corporation has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy statement and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF)

program, and to view our certification, please visit the U.S. Department of Commerce's Data Privacy Framework website. The controlled U.S. subsidiaries of Microsoft Corporation, as identified in our self-certification submission, also adhere to the DPF Principles—for more info, see the list of Microsoft U.S. entities or subsidiaries adhering to the DPF Principles.

If you have a question or complaint related to participation by Microsoft in the DPF Frameworks, we encourage you to contact us via our web form. For any complaints related to the DPF Frameworks that Microsoft cannot resolve directly, we have chosen to cooperate with the relevant EU Data Protection Authority, or a panel established by the European data protection authorities, for resolving disputes with EU individuals, the UK Information Commissioner (for UK individuals), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) for resolving disputes with Swiss individuals. Please contact us if you'd like us to direct you to your data protection authority contacts. As further explained in the DPF Principles, binding

arbitration is available to address residual complaints not resolved by other means. Microsoft is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

Individuals whose personal data is protected by Japan's Act on the Protection of Personal Information should refer to the article on the Japanese Personal Information Protection Commission's website (only published in Japanese) for more information on the commission's review of certain countries' personal data protection systems.

Our retention of personal data

Microsoft retains personal data for as long as necessary to provide the products and fulfill the transactions you have requested, or for other legitimate purposes such as complying with our legal obligations, resolving disputes, and enforcing our agreements. Because these needs can vary for different data types, the context of our interactions with you or your use of products, actual retention periods can vary significantly.

Other criteria used to determine the retention periods include:

- **Do customers provide, create, or maintain the data with the expectation we will retain it until they affirmatively remove it?** Examples include a document you store in OneDrive, or an email message you keep in your Outlook.com inbox. In such cases, we would aim to maintain the data until you actively delete it, such as by moving an email from your Outlook.com inbox to the Deleted Items folder, and then emptying that folder (when your Deleted Items folder is emptied, those emptied items remain in our system for up to 30 days before final deletion). (Note that there may be other reasons why the data has to be deleted sooner, for example if you exceed limits on how much data can be stored in your account.)
- **Is there an automated control, such as in the Microsoft privacy dashboard, that enables the customer to access and delete the personal data at any time?** If there is

not, a shortened data retention time will generally be adopted.

- **Is the personal data of a sensitive type?** If so, a shortened retention time would generally be adopted.
- **Has Microsoft adopted and announced a specific retention period for a certain data type?** For example, for Bing search queries, we de-identify stored queries by removing the entirety of the IP address after 6 months, and cookie IDs and other cross-session identifiers that are used to identify a particular account or device after 18 months.
- **Has the user provided consent for a longer retention period?** If so, we will retain data in accordance with your consent.
- **Is Microsoft subject to a legal, contractual, or similar obligation to retain or delete the data?** Examples can include mandatory data retention laws in the applicable jurisdiction, government orders to preserve data relevant to an investigation, or data retained for the purposes of litigation.

Conversely, if we are required by law to remove unlawful content, we will do so.

U.S. State Data Privacy

If you are a U.S. resident, we process your personal data in accordance with applicable U.S. state data privacy laws, including the California Consumer Privacy Act (CCPA). This section of our privacy statement contains information required by the CCPA and other U.S. state data privacy laws and supplements our privacy statement.

Please note that recent changes to the CCPA and other state data privacy laws are set to take effect in 2023; however, the rules implementing some of these laws have not yet been finalized. We are continuously working to better comply with these laws, and we will update our processes and disclosures as these implementing rules are finalized.

Please also see our U.S. State Data Privacy Laws Notice and our Washington State Consumer Health Data Privacy Policy for additional information about the data we

collect, process, share and disclose, and your rights under applicable U.S. state data privacy laws.

Sale. We do not sell your personal data. So, we do not offer an opt-out to the sale of personal data.

Share. We may "share" your personal data, as defined under California and other applicable U.S. state laws, for personalized advertising purposes. As noted in our Advertising section, we do not deliver personalized advertising to children whose birthdate in their Microsoft account identifies them as under 18 years of age.

In the bulleted list below, we outline the categories of data we share for personalized advertising purposes, the recipients of the personal data, and our purposes of processing. For a description of the data included in each category, please see the Personal data we collect section.

Categories of Personal Data

- Name and contact data

    - Recipients: Third parties that perform online advertising services for Microsoft
    - Purposes of Processing: To deliver personalized advertising based on your interests
- Demographic data
    - Recipients: Third parties that perform online advertising services for Microsoft
    - Purposes of Processing: To deliver personalized advertising based on your interests
- Subscription and licensing data
    - Recipients: Third parties that perform online advertising services for Microsoft
    - Purposes of Processing: To deliver personalized advertising based on your interests
- Interactions
    - Recipients: Third parties that perform online advertising services for Microsoft
    - Purposes of Processing: To deliver personalized advertising based on your interests

Please see the Advertising section for more information about our advertising practices, and our U.S. State Data Privacy Laws Notice for more information on "sharing" for personalized advertising purposes under applicable U.S. state laws.

Rights. You have the right to request that we (i) disclose what personal data we collect, use, disclose, share, and sell, (ii) delete your personal data, (iii) correct your personal data, (iv) restrict the use and disclosure of your sensitive data, and (v) opt-out of "sharing" your personal data with third parties for personalized advertising purposes on third party sites. You may make these requests yourself or through an authorized agent. If you use an authorized agent, we provide your agent with detailed guidance on how to exercise your privacy rights. Please see our U.S. State Data Privacy Laws Notice for additional information on how to exercise these rights. Please also see our Washington State Consumer Health Data Privacy Policy for information on the rights available under Washington law.

If you have a Microsoft account, you can exercise your rights through the Microsoft privacy dashboard, which requires you to log in to your Microsoft account. If you have an additional request or questions after using the dashboard, you may contact Microsoft at the address in the How to contact us section, use our web form, or call our US toll free number +1 (844) 931 2038. If you do not have an account, you may exercise your rights by contacting us as described above. We may ask for additional information, such as your country of residence, email address, and phone number to validate your request before honoring the request.

You may indicate your choice to opt-out of the sharing of your personal data with third parties for personalized advertising on third party sites by visiting our sharing opt-out page. You can also control the personalized advertising you see on Microsoft properties by visiting our opt-out page.

We do not use or disclose your sensitive data for purposes other than those listed below,

without your consent, or as permitted or required under applicable laws. So, we do not offer an ability to limit the use of sensitive data.

You have a right not to receive discriminatory treatment if you exercise your privacy rights. We will not discriminate against you if you exercise your privacy rights.

Personal information processing. In the bulleted list below, we outline the categories of personal data we collect, the sources of the personal data, our purposes of processing, and the categories of third-party recipients with whom we provide the personal data. For a description of the data included in each category, please see the Personal data we collect section. Please see the Our retention of personal data section for information on personal data retention criteria.

Categories of Personal Data

- Name and contact data
  - Sources of personal data: Interactions with users and partners with whom we offer co-branded services

    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide our products; respond to customer questions; help, secure, and troubleshoot; and marketing
    - Recipients: Service providers and user-directed entities
- Credentials
    - Sources of personal data: Interactions with users and organizations that represent users
    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide our products; authentication and account access; and help, secure and troubleshoot
    - Recipients: Service providers and user-directed entities
- Demographic data
    - Sources of personal data: Interactions with users and purchases from data brokers
    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide and

personalize our products; product development; help, secure, and troubleshoot; and marketing
    - Recipients: Service providers and user-directed entities
- Payment data
    - Sources of personal data: Interactions with users and financial institutions
    - Purposes of Processing (Collection and Disclosure to Third Parties): Transact commerce; process transactions; fulfill orders; help, secure, and troubleshoot; and detect and prevent fraud
    - Recipients: Service providers and user-directed entities
- Subscription and licensing data
    - Sources of personal data: Interactions with users and organizations that represent users
    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide, personalize, and activate our products; customer support; help, secure, and troubleshoot; and marketing

    - Recipients: Service providers and user-directed entities
- Interactions
    - Sources of personal data: Interactions with users including data Microsoft generates through those interactions
    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide and personalize our products; product improvement; product development; marketing; and help, secure and troubleshoot
    - Recipients: Service providers and user-directed entities
- Content
    - Sources of personal data: Interactions with users and organizations that represent users
    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide our products; safety; and help, secure, and troubleshoot
    - Recipients: Service providers and user-directed entities

- Video or recordings
  - Sources of personal data: Interactions with users and publicly available sources
  - Purposes of Processing (Collection and Disclosure to Third Parties): Provide our products; product improvement; product development; marketing; help, secure, and troubleshoot; and safety
  - Recipients: Service providers and user-directed entities
- Feedback and ratings
  - Sources of personal data: Interactions with users
  - Purposes of Processing (Collection and Disclosure to Third Parties): Provide our products; product improvement; product development; customer support; and help, secure, and troubleshoot
  - Recipients: Service providers and user-directed entities

While the bulleted list above contains the primary sources and purposes of processing for each category of personal data, we also collect personal data from the sources listed

in the Personal data we collect section, such as developers who create experiences through or for Microsoft products. Similarly, we process all categories of personal data for the purposes described in the How we use personal data section, such as meeting our legal obligations, developing our workforce, and doing research.

Subject to your privacy settings, your consent, and depending on the products you use and your choices, we may collect, process, or disclose certain personal data that qualifies as "sensitive data" under applicable U.S. state data privacy laws. Sensitive data is a subset of personal data. In the list below, we outline the categories of sensitive data we collect, the sources of the sensitive data, our purposes of processing, and the categories of third party recipients with whom we share the sensitive data. Please see the Personal data we collect section for more information about the sensitive data we may collect.

Categories of Sensitive Data

- Account log-in, financial account, debit or credit card number, and the means to access the account (security or access code, password, credentials, etc.)
  - Sources of sensitive data: Interactions with users and organizations that represent users
  - Purposes of Processing (Collection and Disclosure to Third Parties): Provide the product and fulfill requested financial transactions
  - Recipients: Service providers and payment processing providers
- Precise geo-location information
  - Sources of sensitive data: Users' interactions with the products
  - Purposes of Processing (Collection and Disclosure to Third Parties): Provide the service requested; product improvement; some attributes may be disclosed to third parties to provide the service
  - Recipients: Users and service providers (please see the Windows Location Services and Recording section of our privacy statement for more information)

- Racial or ethnic origin, religious or philosophical beliefs, or union membership
  - Sources of sensitive data: Communications with users
  - Purposes of Processing (Collection and Disclosure to Third Parties): Conduct research studies to better understand how our products are used and perceived and for the purposes of improving the product experiences
  - Recipients: Service providers
- Medical or mental health, sex life, or sexual orientation
  - Sources of sensitive data: Communications with users
  - Purposes of Processing (Collection and Disclosure to Third Parties): Conduct research studies to better understand how our products are used and perceived and for the purposes of improving the product experiences and accessibility
  - Recipients: Service providers
- Contents of your mail, email, or text messages (where Microsoft is not the

intended recipient of the communication)
    - Sources of sensitive data: Users' interactions with the products
    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide our products; improve the product experience; safety; and help, secure, and troubleshoot
    - Recipients: Service providers
- Personal data collected from a known child under 13 years of age
    - Sources of sensitive data: Interactions with users and organizations that represent users
    - Purposes of Processing (Collection and Disclosure to Third Parties): Provide our products; product improvement; product development; recommendations; help, secure, and troubleshoot; and safety
    - Recipients: Service providers and user-directed entities (in accordance with your Microsoft Family Safety settings)

While the bulleted list above contains the primary sources and purposes of processing

for personal data collected from children under 13, we also collect personal data from the sources listed in the Collection of Data from Children section.

We do not use or disclose your sensitive data for purposes other than the following:

- Perform the services or provide the goods you reasonably expect
- Help ensure the security and integrity of our services, systems, and data, to combat malicious deceptive, fraudulent or illegal acts, and to protect the physical safety of individuals, to the extent the processing is reasonably necessary and proportionate
- For short-term transient use (including non-personalized advertising), so long as the personal data is not disclosed to a third party, is not used for profiling, and is not used to alter an individual's experience outside the current interaction with Microsoft
- Perform services on behalf of Microsoft, such as maintaining accounts, providing customer service, processing, or fulfilling

orders/transactions, verifying customer information, processing payments, providing financing, providing analytics, providing storage, and similar services
- Undertake activities to verify or maintain the quality or safety of, or improve, upgrade, or enhance a service or device owned or controlled by Microsoft
- Collect or process sensitive data where the collection or processing is not for inferring characteristics about the individual
- Any other activities in accordance with any future regulations that are issued pursuant to U.S. state data privacy laws

De-Identified Data. In some situations, Microsoft may process de-identified data. Data is in this state when we are not able to link data to an individual to whom such data may relate without taking additional steps. In those instances, and unless allowed under applicable law, we will maintain such information in a de-identified state, and will not try to re-identify the individual to whom the de-identified data relates.

Disclosures of personal data for business or commercial purposes. As indicated in the Reasons we share personal data section, we share personal data with third parties for various business and commercial purposes. The primary business and commercial purposes for which we share personal data are the purposes of processing listed in the table above. However, we share all categories of personal data for the business and commercial purposes in the Reasons we share personal data section.

Parties that control collection of personal data. In certain situations, we may allow a third party to control the collection of your personal data. For example, third party applications or extensions that run on Windows or Edge browser may collect personal data based on their own practices.

Microsoft allows advertising companies to collect information about your interactions with our websites in order to deliver personalized ads on Microsoft's behalf. These

companies include: Meta, LinkedIn, Google, and Adobe.

Artificial Intelligence

Microsoft leverages the power of artificial intelligence (AI) in many of our products and services, including by incorporating generative AI features. Microsoft's development and use of AI is subject to Microsoft's AI Principles and Microsoft's Responsible AI Standard, and the collection and use of personal data in developing and deploying AI features is consistent with the commitments outlined in this privacy statement. Product-specific details provide additional relevant information. You can find out more about how Microsoft uses AI here.

Advertising

Advertising allows us to provide, support, and improve some of our products. Microsoft does not use what you say in email, human-to-human chat, video calls or voice mail, or your documents, photos, or other personal files to target ads to you. We use other data, detailed

below, for advertising on our Microsoft properties and on third-party properties. For example:

- Microsoft may use data we collect to select and deliver some of the ads you see on Microsoft web properties, such as Microsoft.com, Microsoft Start, and Bing.
- When the advertising ID is enabled in Windows as part of your privacy settings, third parties can access and use the advertising ID (much the same way that websites can access and use a unique identifier stored in a cookie) to select and deliver ads in such apps.
- We may share data we collect with internal and external partners, such as Xandr, Yahoo, or Facebook (see below), so that the ads you see in our products and their products are more relevant and valuable to you.
- Advertisers may choose to place our web beacons on their sites, or use similar technologies, in order to allow Microsoft to collect information on their sites such as activities, purchases, and visits; we use this

data on behalf of our advertising customers to provide ads.

The ads that you see may be selected based on data we process about you, such as your interests and favorites, your location, your transactions, how you use our products, your search queries, or the content you view. For example, if you view content on Microsoft Start about automobiles, we may show advertisements about cars; if you search “pizza places in Seattle” on Bing, you may see advertisements in your search results for restaurants in Seattle.

The ads that you see may also be selected based on other information learned about you over time using demographic data, location data, search queries, interests and favorites, usage data from our products and sites, and the information we collect about you from the sites and apps of our advertisers and partners. We refer to these ads as "personalized advertising" in this statement. For example, if you view gaming content on xbox.com, you may see offers for games on Microsoft Start.

To provide personalized advertising, we combine cookies placed on your device using information that we collect (such as IP address) when your browser interacts with our websites. If you opt out of receiving personalized advertising, data associated with these cookies will not be used.

We may use information about you to serve you with personalized advertising when you use Microsoft services. If you are logged in with your Microsoft account and have consented to allow Microsoft Edge to use your online activity for personalized advertising, you will see offers for products and services based on your online activity while using Microsoft Edge. To configure your privacy settings for Edge, go to Microsoft Edge > Settings > Privacy and Services. To configure your privacy and ad settings for your Microsoft account with respect to your online activity across browsers, including Microsoft Edge, or when visiting third-party websites or apps, go to your dashboard at privacy.microsoft.com.

Further details regarding our advertising-related uses of data include:

- **Advertising industry best practices and commitments**. Microsoft is a member of the Network Advertising Initiative (NAI) and adheres to the NAI Code of Conduct. We also adhere to the following self-regulatory programs:
  - In the US: Digital Advertising Alliance (DAA)
  - In Europe: European Interactive Digital Advertising Alliance (EDAA)
  - In Canada: Ad Choices: Digital Advertising Alliance of Canada (DAAC) / Choix de Pub: l'Alliance de la publicité numérique du Canada (DAAC)
- **Health-related ad targeting**. In the United States, we provide personalized advertising based on a limited number of standard, non-sensitive health-related interest categories, including allergies, arthritis, cholesterol, cold and flu, diabetes, gastrointestinal health, headache / migraine, healthy eating, healthy heart, men's health, oral health, osteoporosis, skin health, sleep, and vision /

eye care. We will also personalize ads based on custom, non-sensitive health-related interest categories as requested by advertisers.

- **Children and advertising**. We do not deliver personalized advertising to children whose birthdate in their Microsoft account identifies them as under 18 years of age.
- **Data retention**. For personalized advertising, we retain data for no more than 13 months, unless we obtain your consent to retain the data longer.
- **Sensitive Data**. Microsoft Advertising does not collect, process, or disclose personal data that qualifies as “sensitive data” under applicable U.S. state data privacy laws for the purposes of providing personalized advertising.
- **Data sharing**. In some cases, we share with advertisers reports about the data we have collected on their sites or ads.

Data collected by other advertising companies. Advertisers sometimes include their own web beacons (or those of their other advertising partners) within their

advertisements that we display, enabling them to set and read their own cookie. Additionally, Microsoft partners with Xandr, a Microsoft company, and third-party ad companies to help provide some of our advertising services, and we also allow other third-party ad companies to display advertisements on our sites. These third parties may place cookies on your computer and collect data about your online activities across websites or online services. These companies currently include, but are not limited to: Facebook, Media.net, Outbrain, Taboola and Yahoo. Select any of the preceding links to find more information on each company's practices, including the choices it offers. Many of these companies are also members of the NAI or DAA, which each provide a simple way to opt out of ad targeting from participating companies.

To opt out of receiving personalized advertising from Microsoft, visit our opt-out page. When you opt out, your preference is stored in a cookie that is specific to the web browser you are using. The opt-out cookie has an expiration date of five years. If you delete

the cookies on your device, you need to opt out again.

Speech recognition technologies

Speech recognition technologies are integrated into many Microsoft products and services. Microsoft provides both device-based speech recognition features and cloud-based (online) speech recognition features. Microsoft's speech recognition technology transcribes voice data into text. With your permission, Microsoft employees and vendors working on behalf of Microsoft, will be able to review snippets of your voice data or voice clips in order to build and improve our speech recognition technologies. These improvements allow us to build better voice-enabled capabilities that benefit users across all our consumer and enterprise products and services. Prior to employee or vendor review of voice data, we protect users' privacy by taking steps to de-identify the data, requiring non-disclosure agreements with relevant vendors and their employees, and requiring that employees and vendors meet high privacy

standards. Learn more about Microsoft and your voice data.

Preview or free-of-charge releases

Microsoft offers preview, insider, beta or other free-of-charge products and features ("previews") to enable you to evaluate them while providing Microsoft with data about your use of the product, including feedback and device and usage data. As a result, previews can automatically collect additional data, provide fewer controls, and otherwise employ different privacy and security measures than those typically present in our products. If you participate in previews, we may contact you about your feedback or your interest in continuing to use the product after general release.

Changes to this privacy statement

We update this privacy statement when necessary to provide greater transparency or in response to:

- Feedback from customer, regulators, industry, or other stakeholders.
- Changes in our products.
- Changes in our data processing activities or policies.

When we post changes to this statement, we will revise the "last updated" date at the top of the statement and describe the changes on the Change history page. If there are material changes to the statement, such as a change to the purposes of processing of personal data that is not consistent with the purpose for which it was originally collected, we will notify you either by prominently posting a notice of such changes before they take effect or by directly sending you a notification. We encourage you to periodically review this privacy statement to learn how Microsoft is protecting your information.

How to contact us

If you have a privacy concern, complaint, or question for the Microsoft Chief Privacy Officer or the Data Protection Officer for your region, please contact us by using our web form. We

will respond to questions or concerns as required by law and within a period no longer than 30 days. You can also raise a concern or lodge a complaint with a data protection authority or other official with jurisdiction.

When Microsoft is a controller, unless otherwise stated, Microsoft Corporation and, for those in the European Economic Area, the United Kingdom, and Switzerland, Microsoft Ireland Operations Limited are the data controllers for personal data we collect through the products subject to this statement. Our addresses are:

- Microsoft Privacy, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, USA. Telephone: +1 (425) 882 8080.
- Microsoft Ireland Operations Limited, Attn: Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland. Telephone: +353 1 706 3117.

To find the Microsoft subsidiary in your country or region, see the list of Microsoft office locations around the world.

If you would like to exercise your rights under applicable U.S. state data privacy law, you may contact Microsoft at the address above, use our web form, or call our U.S. toll free number +1 (844) 931 2038.

If you are a resident of Canada and its provinces you may contact the Microsoft Data Protection Officer for Canada at Microsoft, 1950 Meadowvale Blvd, Mississauga, Ontario, L5N 8L9, at +1 (416) 349 2506, or by using our web form.

Where French law applies, you can also send us specific instructions regarding the use of your personal data after your death, by using our web form.

If you have a technical or support question, please visit Microsoft Support to learn more about Microsoft Support offerings. If you have a personal Microsoft account password question, please visit Microsoft account support.

We offer various means for you to control your personal data that Microsoft has obtained, and to exercise your data protection rights. You

can do so by contacting Microsoft at our web form or the information above, or by using the various tools we provide. Please see the How to access and control your personal data section for additional details.

Enterprise and developer products

Enterprise and Developer Products are Microsoft products and related software offered to and designed primarily for use by organizations and developers. They include:

- Cloud services, referred to as Online Services in the Product Terms, such as Microsoft 365 and Office 365, Microsoft Azure, Microsoft Dynamics365, and Microsoft Intune for which an organization (our customer) contracts with Microsoft for the services ("Enterprise Online Services").
- Other enterprise and developer tools and cloud-based services, such as Azure PlayFab Services (to learn more see Azure PlayFab Terms of Service).
- Server, developer, and hybrid cloud platform products, such as Windows Server, SQL Server, Visual Studio, System Center, Azure Stack and

open source software like Bot Framework solutions (“Enterprise and Developer Software”).
- Appliances and hardware used for storage infrastructure, such as StorSimple (“Enterprise Appliances”).
- Professional services referred to in the Product Terms that are available with Enterprise Online Services, such as onboarding services, data migration services, data science services, or services to supplement existing features in the Enterprise Online Services.

In the event of a conflict between this Microsoft privacy statement and the terms of any agreement(s) between a customer and Microsoft for Enterprise and Developer Products, the terms of those agreement(s) will control.

You can also learn more about our Enterprise and Developer Products’ features and settings, including choices that impact your privacy or your end users’ privacy, in product documentation.

If any of the terms below are not defined in this Privacy Statement or the Product Terms, they have the definitions below.

General. When a customer tries, purchases, uses, or subscribes to Enterprise and Developer Products, or obtains support for or professional services with such products, Microsoft receives data from you and collects and generates data to provide the service (including improving, securing, and updating the service), conduct our business operations, and communicate with the customer. For example:

- When a customer engages with a Microsoft sales representative, we collect the customer's name and contact data, along with information about the customer's organization, to support that engagement.
- When a customer interacts with a Microsoft support professional, we collect device and usage data or error reports to diagnose and resolve problems.
- When a customer pays for products, we collect contact and payment data to process the payment.
- When Microsoft sends communications to a customer, we use data to personalize the content of the communication.

- When a customer engages with Microsoft for professional services, we collect the name and contact data of the customer's designated point of contact and use information provided by the customer to perform the services that the customer has requested.

The Enterprise and Developer Products enable you to purchase, subscribe to, or use other products and online services from Microsoft or third parties with different privacy practices, and those other products and online services are governed by their respective privacy statements and policies.

Enterprise online services

To provide the Enterprise Online Services, Microsoft uses data you provide (including Customer Data, Personal Data, Administrator Data, Payment Data, and Support Data) and data Microsoft collects or generates associated with your use of the Enterprise Online Services. We process data as described in the Product Terms, Microsoft Products and Services Data Protection Addendum (Products and Services DPA), and the Microsoft Trust Center.

Personal Data. Customer is the controller of Personal Data and Microsoft is the processor of such data, except when (a) Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor or (b) as stated otherwise in the standard Products and Services DPA. In addition, as provided in the standard Products and Services DPA, Microsoft has taken on the added responsibilities of a data controller under GDPR when processing Personal Data in connection with its business operations incident to providing its services to Microsoft's commercial customers, such as billing and account management; compensation; internal reporting and business modeling; and financial reporting. We use Personal Data in the least identifiable form that will support processing necessary for these business operations. We rely on statistical data and aggregate pseudonymized Personal Data before using it for our business operations, removing the ability to identify specific individuals.

Administrator Data. Administrator Data is the information provided to Microsoft during sign-

up, purchase, or administration of Enterprise Online Services. We use Administrator Data to provide the Enterprise Online Services, complete transactions, service the account, detect and prevent fraud, and comply with our legal obligations. Administrator Data includes the name, address, phone number, and email address you provide, as well as aggregated usage data related to your account, such as the controls you select. Administrator Data also includes contact information of your colleagues and friends if you agree to provide it to Microsoft for the limited purpose of sending them an invitation to use the Enterprise Online Services; we contact those individuals with communications that include information about you, such as your name and profile photo.

As needed, we use Administrator Data to contact you to provide information about your account, subscriptions, billing, and updates to the Enterprise Online Services, including information about new features, security, or other technical issues. We also contact you regarding third-party inquiries we receive

regarding use of the Enterprise Online Services, as described in your agreement. You cannot unsubscribe from these non-promotional communications. We may also contact you regarding information and offers about other products and services, or share your contact information with Microsoft's partners. When such a partner has specific services or solutions to meet your needs, or to optimize your use of the Enterprise Online Services, we may share limited, aggregated information about your organization’s account with the partner. Microsoft will not share your confidential information or contact information with the authorized partner unless we have sufficient rights to do so. You can manage your contact preferences or update your information in your account profile.

Payment Data. We use payment data to complete transactions, as well as to detect and prevent fraud.

Support Data. Customers provide or authorize Microsoft to collect data in connection with obtaining technical support for the Enterprise

Online Services. We process Support Data to provide technical support and as described in the Products and Services DPA.

Local Software and Diagnostic Data. Some Online Services may require, or may be enhanced by, the installation of local software (e.g., agents, device management applications). The local software may collect Diagnostic Data (as defined in the Products and Services DPA) about the use and performance of that software. That data may be transmitted to Microsoft and used for the purposes described in the Products and Services DPA.

Bing Search Services Data. Bing Search Services, as defined in the Product Terms, use data such as search queries as described in the Bing section of this privacy statement.

Enterprise and developer software and enterprise appliances

Enterprise and developer software and enterprise appliances collect data to operate effectively and provide you the best

experiences. The data we collect depends on the features you use, as well as your configuration and settings, but it is generally limited to device and usage data. Customers have choices about the data they provide. Here are examples of the data we collect:

- During installation or when you upgrade an enterprise and developer software, we may collect device and usage data to learn whether you experience any difficulties.
- When you use enterprise software or enterprise appliances, we may collect device and usage data to learn about your operating environment to improve security features.
- When you experience a crash using enterprise software or enterprise appliances, you may choose to send Microsoft an error report to help us diagnose the problem and deliver customer support.

Microsoft uses the data we collect from enterprise and developer software and enterprise appliances to provide and improve

our products, to deliver customer support, to activate the product, to communicate with you, and to operate our business.

Microsoft SQL Server is a relational database management platform and includes products that can be installed separately (such as SQL Server Management Studio). For detailed information about what data we collect, how we use it, and how to manage your privacy options, visit the SQL Server privacy page. If you work in an organization, your administrator can set certain telemetry settings in SQL Server via Group Policy.

HoloLens. HoloLens headsets are self-contained Windows computers with Wi-Fi connectivity that enable a mixed reality experience for apps and solutions. Microsoft collects diagnostic data to solve problems and to keep Windows running on HoloLens up to date, secure, and operating properly. Diagnostic data also helps us improve HoloLens and related Microsoft products and services depending on the diagnostic data

settings you've chosen for your device. Learn more about Windows diagnostic data.

HoloLens also processes and collects data related to the HoloLens experience and device, which include cameras, microphones, and infrared sensors that enable motions and voice to navigate.

- If you choose, cameras can be used to sign you in automatically using your iris. To do this, HoloLens takes an image of your iris and measures distances between key points to create and store a numeric value that represents only you. This data stays on the HoloLens and is not shared with anyone, and you can choose to delete this data from your HoloLens at any time.
- HoloLens also detects hand gestures intended for system interactions (such as menu navigation, pan/zoom, and scroll). This data is processed on your HoloLens device and is not stored.
- HoloLens derives tracking points based on your environment which allows it to understand surfaces in space and allows

you to place digital assets on them. There are no images associated with this environmental data and it is stored locally on the HoloLens device. You can choose to delete this data from your HoloLens at any time.

The headset's microphones enable voice commands for navigation, controlling apps, or to enter search terms. Learn more about voice data collection.

Productivity and communications products

Productivity and communications products are applications, software, and services you can use to create, store, and share documents, as well as communicate with others.

Microsoft 365 and Office

Microsoft 365, previous versions called Office 365, is a collection of subscription productivity services and applications including Word, Excel, PowerPoint, and Outlook, among others. Office is the one-time purchase version of these applications available on PC or Mac.

Both Microsoft 365 and Office are comprised of client software applications and connected online services (or web apps in the case of Microsoft 365 for the web) that span many platforms and have numerous interdependent experiences. For more details about Outlook, see the Outlook section of this privacy statement.

Various cloud-based Microsoft 365 services enable you to use your file content for designs and recommendations, collaborate with others within your documents, and provide you functionality from other Microsoft products, such as Bing and Cortana, and third-party connected products. If you work in an organization, your administrator may turn off or disable these connected services. You can access the privacy controls within your Microsoft 365 and Office apps. For more information, see Account Privacy Settings.

Office Roaming Service. The Office Roaming Service helps keep your settings, including your privacy settings, up to date across your devices running Microsoft 365 or Office apps.

When you sign in to your apps with either your Microsoft account or an account issued by your organization, the service syncs some of your customized settings to Microsoft servers. For example, the service syncs a list of most recently used documents or the last location viewed within a document. When you sign in to another device with the same account, the Office Roaming Service downloads your settings from Microsoft servers and applies them to the additional device. When you sign out of your apps, the service removes your settings from your device. Any changes you make to your customized settings are sent to Microsoft servers.

Updates from Microsoft. Microsoft uses services such as Click-to-Run, Microsoft AutoUpdate (for Mac), or Microsoft Update (for some versions of Office) to provide you with security and other important updates.

These services can automatically detect the availability of online updates for Microsoft 365 or Office apps on your device and download and install them automatically.

Diagnostic Data. Diagnostic data is used to (i) keep your Microsoft 365 or Office apps secure and up to date; (ii) detect, diagnose, and remediate problems; and (iii) make product improvements. This data does not include a user's name or email address, the content of the user's files, or information about apps unrelated to Microsoft 365 or Office. Users have a choice between two different levels of diagnostic data collection, Required and Optional.

- **Required**. The minimum data necessary to help keep apps secure, up to date, and performing as expected on the device it's installed on.
- **Optional**. Additional data that helps us make product improvements and provides enhanced information to help us detect, diagnose, and remediate issues.

See Diagnostic Data for more information.

Connected Experiences. Microsoft 365 continues to provide more experiences in client applications that are connected to and backed by cloud-based services. A subset of

these connected experiences is also available in Office. If you choose to use connected experiences, required service data will be collected to help keep these connected experiences reliable, up to date, secure, and performing as expected. See below for additional information about required service data.

Working with others on a document stored on OneDrive or translating the contents of a Word document into a different language are examples of connected experiences. There are two types of connected experiences.

- **Experiences that analyze your content**. Experiences that use your file content to provide you with design recommendations, editing suggestions, data insights, and similar features. For example, PowerPoint Designer or Editor in Word.
- **Experiences that download online content**. Experiences that allow you to search and download online content including templates, images, 3D models, videos, and reference materials to enhance your

documents. For example, templates or PowerPoint QuickStarter.

You can access the privacy controls within your Microsoft 365 and Office client apps. These privacy settings allow you to configure your connected experiences. For example, you can choose to enable connected experiences that download online content, but not connected experiences that analyze content. Turning off connected experiences will also turn off additional experiences, such as document co-authoring and online file storage. But even if you use this privacy setting to turn off connected experiences, certain functionality will remain available, such as syncing your mailbox in Outlook, as well as essential services described below. These controls are not available when using Microsoft 365 for the web, since you will already be cloud-connected. For more information about accessing these controls, see Account Privacy Settings.

If you choose to disable certain types of connected experiences, either the ribbon or

menu command for those connected experiences will be grayed out or you will get an error message when you try to use those connected experiences.

Essential services. There are a set of services that are essential to how Microsoft 365 and Office functions and cannot be disabled. For example, the licensing service that confirms that you are properly licensed to use Microsoft 365 is essential. Required service data about these services is collected and sent to Microsoft, regardless of any other settings that you have configured. See Essential Services for more information.

Required service data for connected experiences. As you use a connected experience, data is sent to and processed by Microsoft to provide you that connected experience. This data is necessary because this information enables us to deliver these cloud-based connected experiences. We refer to this data as required service data.

Required service data can include information related to the operation of the connected

experience that is needed to keep the underlying service secure, up to date, and performing as expected. If you choose to use a connected experience that analyzes your content, for example Translate in Word, the text you typed and selected to translate is also sent and processed to provide you the connected experience. Your text and the translation are not stored by our service. Required service data can also include information needed by a connected experience to perform its task, such as configuration information about the Microsoft 365 or Office app.

See Required service data for more information.

Microsoft Family

This section applies to the Microsoft Family Safety M365 product, which allows a family group to connect through the Microsoft Family Safety app on their Windows, Xbox, or mobile devices. Please carefully review the information at Microsoft Family Safety if choosing to create or join a family group.

Microsoft Family Safety can help parents and guardians to create a safer environment for their family group with digital content filtering, screen time limits, spending for Microsoft and Xbox stores, setting age ratings for apps and games, and location sharing. To learn about how Microsoft collects and uses children's data, see the Collection of data from children section of the Privacy Statement. If you are using Microsoft Family Safety in Windows, see the Windows security and safety features section of the Privacy Statement for additional information.

When you have enabled family activity reporting for a child, Microsoft will collect details about how the child uses their devices, such as search, web, app, and game activity, and provide parents with reports of that child's online activities. Activity reports are routinely deleted from Microsoft servers.

Certain Family Safety features, such as Location Sharing, Drive Safety, Share Drives, Places, and Location Alerts will use your location information when enabled. When you

have enabled Location Sharing, for instance, your device will upload location data to the cloud and share it with others in your family group. Microsoft retains only your last known location as part of the Location Sharing feature (each new location replaces the previous one). When you enable Drive Safety, your location will be used to record your drive habits such as whether you are driving within the speed limits, if you're using your phone while driving, and if you accelerate or brake suddenly. These reports will be uploaded to the cloud, and you can choose to share your drive reports with your family group. You can turn off these location features at any time in the Family Safety settings. You can manage your device's location data at the Microsoft Privacy Dashboard. Learn more about Family Safety and your location data.

Microsoft Teams

This section applies to the consumer offering of Teams; if you are using Teams with a school or work account, see the Enterprise and developer products of this privacy statement.

Teams is an all-in-one collaboration and communication hub. Teams lets you stay organised and connected across your entire life. Teams allows you to call people with voice or video calling. Teams allows you to easily find people, files, photos, conversations, tasks, and calendars in one convenient and secure place. Teams allows you to store confidential information like passwords, rewards numbers, or login information and share it with others within Teams. With your consent, you can share your location with friends and family.

As part of providing these features, Microsoft collects data about the usage of the features as well as information about your communications, including the time and date of the communication and users that are part of the communication.

Teams profile. Your Teams profile includes information you provided when you set up a Microsoft account. To enable other people to find you on Teams (or products that interact with Teams for personal use, including Teams for enterprise) your display name and picture

are visible to other users on Teams that have your contact information.

Teams contacts. With your permission, Teams will sync your device, Outlook, and Skype contacts periodically and check for other Teams users that match contacts in your device, Outlook, or Skype address books. You are always in control of your contacts and can stop syncing at any time. If you choose to stop syncing your device, Outlook, or Skype contacts, or you are inactive on your device, any contacts that have not been matched during the synchronization process will be deleted from Teams. If you wish to invite any of your device, Outlook, or Skype contacts to join a conversation, you can invite users to a 1:1 directly, or Microsoft can send an invitation on your behalf via SMS or email for invitations to group conversations. You can block users if you do not want to receive their communications; additionally, you can report a concern to Microsoft.

Notice to non-user contacts. If your information appears in the device, Outlook, or

Skype address books of a Teams user who chooses to sync their device, Outlook, or Skype contacts with their Teams contacts, Microsoft may process your data in order to determine whether you are a current Teams user and to allow Teams users to invite you to the service, including via SMS and email. As long as the Teams user continues to be active on Teams on their device and continues to enable contact syncing with the applicable device or service, your information will be stored on our servers and we will periodically process your information as a part of the Teams user's contact syncing experience to check whether you have subsequently joined Teams.

Learn more about how we process your information in connection with the contact syncing feature offered to Teams users.

If you do choose to join Teams, you will appear as a suggested new Teams contact for any Teams users with your information in their device, Outlook, or Skype address books. As a Teams user, you will be able to block other Teams users if you do not want to receive their

communications; additionally, you can report a concern to Microsoft.

Third-party contacts. You can also choose to sync contacts from third-party providers. If you choose to unsync your third-party contacts on Teams, all third-party contacts are deleted from Teams. If you gave your consent to use those third-party contacts on other Microsoft apps and services, these contacts will still be available to those other Microsoft apps and services.

You can remove third-party contacts from all Microsoft apps and services by removing third-party accounts from Teams. Please note that removing a third-party account from Teams may impact your experiences on other Microsoft apps and services that also use that third-party account.

Teams calendar. You can also choose to sync your Teams calendar with calendars from third-party providers. You can stop syncing your Teams calendar anytime by removing a third-party account from Teams. If you have consented to use third-party data on other

Microsoft apps and services, please note that removing this third-party account data in Teams may impact your experiences on other Microsoft apps and services.

Location sharing. You can share your static or live location with individuals or groups within Teams. You are in control and can stop sharing at any time. Sharing location for children is permitted with parental consent and in groups where an adult from the Microsoft family group is present.

Push notifications. To let you know of incoming calls, chats, and other messages, Teams uses the notification service on your device. For many devices, these services are provided by another company. To tell you who is calling, for example, or to give you the first few words of the new chat, Teams has to tell the notification service so that they can provide the notification to you. The company providing the notification service on your device will use this information in accordance with their own terms and privacy policy. Microsoft is not responsible for the data

collected by the company providing the notification service.

If you do not want to use the notification services for incoming Teams calls and messages, turn it off in the settings found on your device.

OneDrive

OneDrive lets you store and access your files on virtually any device. You can also share and collaborate on your files with others. Some versions of the OneDrive application enable you to access both your personal OneDrive by signing in with your personal Microsoft account and your OneDrive for Business by signing in with your work or school Microsoft account as part of your organization's use of Microsoft 365 or Office 365.

When you use OneDrive, we collect data about your usage of the service, as well as the content you store, to provide, improve, and protect the services. Examples include indexing the contents of your OneDrive documents so that you can search for them

later and using location information to enable you to search for photos based on where the photo was taken. We also collect device information so we can deliver personalized experiences, such as enabling you to sync content across devices and roam customized settings.

When you store content in OneDrive, that content will inherit the sharing permissions of the folder in which you store it. For example, if you decide to store content in the public folder, the content will be public and available to anyone on the internet who can find the folder. If you store content in a private folder, the content will be private.

When you share content to a social network like Facebook from a device that you have synced with your OneDrive account, your content is either uploaded to that social network, or a link to that content is posted to that social network. Doing this makes the content accessible to anyone on that social network. To delete the content, you need to delete it from the social network (if it was

uploaded there, rather than a link to it) and from OneDrive.

When you share your OneDrive content with your friends via a link, an email with the link is sent to those friends. The link contains an authorization code that allows anyone with the link to access your content. If one of your friends sends the link to other people, they will also be able to access your content, even if you did not choose to share the content with them. To revoke permissions for your content on OneDrive, sign in to your account and then select the specific content to manage the permission levels. Revoking permissions for a link effectively deactivates the link. No one will be able to use the link to access the content unless you decide to share the link again.

Files managed with OneDrive for Business are stored separately from files stored with your personal OneDrive. OneDrive for Business collects and transmits personal data for authentication, such as your email address and password, which will be transmitted to

Microsoft and/or to the provider of your Microsoft 365 or Office 365 service.

Outlook

Outlook products are designed to improve your productivity through improved communications and include Outlook.com, Outlook applications, and related services.

Outlook.com. Outlook.com is the primary consumer email service from Microsoft and includes email accounts with addresses that end in outlook.com, live.com, hotmail.com, and msn.com. Outlook.com provides features that let you connect with your friends on social networks. You will need to create a Microsoft account to use Outlook.com.

When you delete an email or item from a mailbox in Outlook.com, the item generally goes into your Deleted Items folder where it remains for approximately 7 days unless you move it back to your inbox, you empty the folder, or the service empties the folder automatically, whichever comes first. When the Deleted Items folder is emptied, those

emptied items remain in our system for up to 30 days before final deletion, unless we are legally required to retain the data for longer.

Outlook applications. Outlook client applications are software you install on your device that permits you to manage email, calendar items, files, contacts, and other data from email, file storage, and other services, like Exchange Online or Outlook.com, or servers, like Microsoft Exchange. You can use multiple accounts from different providers, including third-party providers, with Outlook applications.

To add an account, you must provide permission for Outlook to access data from the email or file storage services.

When you add an account to Outlook, your mail, calendar items, files, contacts, settings and other data from that account will automatically sync to your device. If you are using the mobile Outlook application, that data will also sync to Microsoft servers to enable additional features such as faster search, personalized filtering of less important mail,

and an ability to add email attachments from linked file storage providers without leaving the Outlook application. If you are using the desktop Outlook application, you can choose whether to allow the data to sync to our servers. At any time, you can remove an account or make changes to the data that is synced from your account.

If you add an account provided by an organization (such as your employer or school), the owner of the organizational domain can implement policies and controls (for example, requiring multi-factor authentication or the ability to remotely wipe data from your device) that can affect your use of Outlook.

To learn more about the data the Outlook applications collect and process, please see the Microsoft 365 section of this privacy statement.

Skype

Skype lets you send and receive voice, video, SMS, and instant message communications.

This section applies to the consumer version of Skype; if you are using Skype for Business, see the Enterprise and developer products section of this privacy statement.

As part of providing these features, Microsoft collects usage data about your communications that includes the time and date of the communication and the numbers or user names that are part of the communication.

Skype profile. Your Skype profile includes information you provided when you set up a Microsoft account. To enable other people to find you on Skype (or products that interact with Skype, such as Skype for Business), depending on your profile settings, your Skype profile is included in the Skype public search. Your profile includes your user name, avatar, and any other data you choose to add to your profile or display to others.

Emergency calling in the United States. If you enable location sharing for emergency calling, your location will be periodically collected to enable Microsoft to share your location with

emergency calling service providers if you dial 911. Your location information is only shared if you enable location sharing for emergency calling and you initiate a 911 call.

Skype contacts. If you use Outlook.com to manage contacts, Skype will automatically add the people you know to your Skype contact list until you tell the application to stop. With your permission, Skype will sync your device contacts periodically and check for other Skype users that match contacts in your device or Outlook address books. You are always in control of your contacts and can stop syncing at any time. You can block users if you do not want to receive their communications. If you choose to stop syncing your device contacts, or you are inactive on your device, any contacts that have not been matched during the synchronization process will be deleted from Skype. If you wish to invite any of your device or Outlook contacts to join a conversation, you can invite users to a 1:1 directly, or Microsoft can send an invitation on your behalf via SMS or email for invitations to group conversations. You can block users if

you do not want to receive their communications; additionally, you can report a concern to Microsoft.

Notice to non-user contacts. If your information appears in the device or Outlook address book of a Skype user who chooses to sync their device or Outlook contacts with their Skype contacts, Microsoft may process your data in order to determine whether you are a current Skype user and to allow Skype users to invite you to the service, including via SMS and email. As long as the Skype user continues to be active on Skype on their device and continues to enable contact syncing, your information will be stored on our servers and we will periodically process your information as a part of the Skype user's contact synching experience to check whether you have subsequently joined Skype.

Learn more about how we process your information in connection with the contact syncing feature offered to Skype users.

If you do choose to join Skype, you will appear as a suggested new Skype contact for any

Skype users with your information in their device or Outlook address books. As a Skype user, you will be able to block other Skype users if you do not want to receive their communications; additionally, you can report a concern to Microsoft.

Partner companies. To make Skype available to more people, we partner with other companies to allow Skype to be offered via those companies' services. If you use Skype through a company other than Microsoft, that company's privacy policy governs how it handles your data. To comply with applicable law or respond to valid legal process, or to help our partner company or local operator comply or respond, we may access, transfer, disclose, and preserve your data. That data could include, for example, your private content, such as the content of your instant messages, stored video messages, voicemails, or file transfers.

Skype Manager. Skype Manager lets you manage a group's (such as your family's) Skype usage from one central place. When you

set up a group, you will be the Skype Manager Administrator and can see the patterns of usage, including detailed information, like traffic data and details of purchases, of other members of the group who have consented to such access. If you add information like your name, other people in the group will be able to see it. Members of the group can withdraw consent for Skype Manager by visiting their Skype account page.

Push notifications. To let you know of incoming calls, chats, and other messages, Skype apps use the notification service on your device. For many devices, these services are provided by another company. To tell you who is calling, for example, or to give you the first few words of the new chat, Skype has to tell the notification service so that they can provide the notification to you. The company providing the notification service on your device will use this information in accordance with their own terms and privacy policy. Microsoft is not responsible for the data collected by the company providing the notification service. If you do not want to use

the notification services for incoming Skype calls and messages, turn it off in the settings found in the Skype application or your device.

Translation features. When you use Skype's translation features, Skype collects and uses your conversation to provide the translation service. With your permission, your data may be used to help improve Microsoft products and services. To help the translation and speech recognition technology learn and grow, sentences and automatic transcripts are analyzed and any corrections are entered into our system, to build better performing services. This data may include manual transcription of your voice clips. To learn more about how Microsoft manages your voice data, see Speech recognition technologies.

Recording features. Some versions of Skype have a recording feature that allows you to capture and share all or part of your audio / video call. The recording will be stored and shared as part of your conversation history with the person or group with whom the call occurred. **You should understand your legal**

responsibilities before recording any communication. This may include obtaining the prior consent of everyone participating in the conversation or any other authorizations as required. Microsoft is not responsible for how you use your recordings or the recording features.

Skype bots. Bots are programs offered by Microsoft or third parties that can do many useful things like search for news, play games, and more. Depending on their capabilities, bots may have access to your display name, Skype ID, country, region, language, and any messages, audio, video, or content that you share with the bot. Please review the bot profile and its privacy statement before engaging in a one-to-one or group conversation with a bot. You can delete a bot that you no longer wish to engage with. Prior to adding a bot to a group, please ensure that your group participants have consented to their information being shared with the bot.

Captioning. Certain Skype features include accessibility functionality such as captioning.

During Skype calls, a call participant can activate a voice-to-text feature, which allows the user to view the audio chat as text. If a user activates this feature, other call participants will not receive a notification. Microsoft uses this voice and text data to provide captioning of audio for users.

Surface Duo

The Surface Duo is a device featuring two screens that fits in your pocket for productivity on the go. Powered by the Google Android operating system, Surface Duo supports cellular and Wi-Fi connectivity and can be used for email, internet browsing, games, and business connectivity.

Microsoft provides a core Surface Duo experience that runs on the Android operating system. The core Surface Duo experience includes apps such as the Microsoft Launcher, Setup Wizard, and Your Phone Companion. You can sign in with a Google ID and enable various Google services; you can then also sign in with your Microsoft account (MSA) and enable Microsoft’s services. Microsoft apps

and services may rely on information provided by Google. Some features, such as location, require that you enable this functionality for Google and separately allow Microsoft to leverage this information.

Diagnostic data. Surface Duo collects diagnostic data to solve problems and to keep the core Surface Duo experience up to date, secure, and operating properly. This data also helps us improve Surface Duo and related Microsoft products and services. The data does not include your user name, email address, or the content of your files. There are two levels of diagnostic data: Required diagnostic data and Optional diagnostic data.

- **Required**. The minimum data necessary to help keep the core Surface Duo experience secure, up to date, and performing as expected.
- **Optional**. Additional data that helps us make product improvements and provides enhanced information to help Microsoft detect, diagnose, and remediate issues.

Learn more in Surface Duo Privacy Settings.

Surface Duo location settings. Surface Duo relies on Google location services to determine the device's precise geographic location to display the local weather. The location of your Surface Duo can be determined with varying degrees of accuracy and may in some cases be determined precisely. If you want Microsoft apps to be able to reference or display weather or other location related information, you need to enable Google location services and Microsoft location access. Some apps may require these settings be enabled independently for the app and can be set or changed in the Surface Duo's Settings. The Google Privacy Policy provides details about Google's location service and related data privacy practices. See Surface Duo Location Settings for more information.

Microsoft apps included with the Surface Duo. The diagnostic data options for the core Surface Duo experience are configured when you initially set up your Surface Duo and can be changed in the Surface Duo's Settings under the Diagnostic Data section.

The other Microsoft apps on your Surface Duo may prompt you to enable functionality to enable the full experience of the app or you may be asked to allow optional diagnostic data collection. You can change the settings for these apps in the Surface Duo Settings under the app name. More information about these apps is available in the Productivity and communications products and Search, Microsoft Edge, and artificial intelligence sections of this Privacy Statement.

LinkedIn

To learn about the data LinkedIn collects and how it is used and shared, please see LinkedIn's Privacy Policy.

Search, Microsoft Edge, and artificial intelligence

Search and artificial intelligence products connect you with information and intelligently sense, process, and act on information—learning and adapting over time.

Bing

Bing services include search and mapping services, as well as other apps and programs described in this section. Bing services collect and process data in many forms, including text that has been inked or typed, voice data, and images. Bing services are also included within other Microsoft services, such as Microsoft 365, Cortana, and certain features in Windows (which we refer to as Bing-powered experiences).

When you conduct a search, or use a feature of a Bing-powered experience that involves conducting a search or entering a command on your behalf, Microsoft will collect the searches or commands you provide (which may be in the form of text, voice data, or an image), along with your IP address, location, the unique identifiers contained in our cookies or similar technologies, the time and date of your search, and your browser configuration. For example, if you use Bing voice-enabled services, your voice input and performance data associated with the speech functionality will be sent to Microsoft. To learn more about

how Microsoft manages your voice data, see Speech recognition technologies. And, if you use Bing image-enabled services, the image you provide will be sent to Microsoft. When you use Bing-powered experiences, such as Bing Lookup to search a particular word or phrase within a webpage or document, that word or phrase is sent to Bing along with some surrounding content in order to provide contextually relevant search results.

AI-powered Bing search. Bing search now includes an AI-enhanced web search functionality, Bing Chat, which supports users by providing relevant search results, reviewing and summarizing from across the web, refining research queries through the chat experience, and sparking creativity by helping users create content. Bing Chat's use and collection of personal data is consistent with Bing's core web search offering as described in this section. More information about the new Bing experience is available at The New Bing: Our approach to Responsible AI.

Search suggestions. For the search suggestions feature, the characters that you type into a Bing-powered experience (such as search and site suggestions in the Microsoft Edge browser) to conduct a search and what you click on will be sent to Microsoft. This allows us to provide you with relevant suggestions as you type your searches. To turn this feature on or off, while using Bing Search, go to Bing Settings. There are other methods to control this feature in other Bing-powered experiences, such as the Microsoft Edge browser. Search Suggestions cannot be turned off in the search box in Windows 10 and Windows 11. If you choose, you can always hide the search box or icon on the taskbar.

Bing experience improvement program for Bing Desktop and Bing Toolbar. If you are using Bing Desktop or Bing Toolbar and choose to participate in the Bing Experience Improvement Program, we also collect additional data about how you use these specific Bing apps, such as the addresses of the websites you visit, to help improve search

ranking and relevance. To help protect your privacy, we do not use the data collected through the Bing Experience Improvement Program to identify or contact you or target advertising to you. You can turn off the Bing Experience Improvement Program at any time in the Bing Desktop or Bing Toolbar settings. Finally, we delete the information collected through the Bing Experience Improvement Program after 18 months.

Retention and de-identification. We de-identify stored search queries by removing the entirety of the IP address after 6 months, and cookie IDs and other cross-session identifiers that are used to identify a particular account or device after 18 months.

Personalization through Microsoft account. Some Bing services provide you with an enhanced experience when you sign in with your personal Microsoft account, for example, syncing your search history across devices. You can use these personalization features to customize your interests, favorites, and settings, and to connect your account with

third-party services. Visit Bing Settings to manage your personalization settings, or the Microsoft privacy dashboard to manage your data.

Managing search history. When you're signed-in to a personal Microsoft account, you can erase your search and chat history on the Microsoft privacy dashboard. The Search History service from Bing, located in Bing Settings, provides another method of revisiting the search terms you've entered and results you've clicked when using Bing search through your browser. You may clear your search history on a device through this service. The conversations you have with Bing chat are also remembered as "Recent activity". The history of previous Recent activities is saved, with the names of chats based by default on the first query of the chat. Your Recent activity is displayed on the right-hand side of the chat window when you are using the service. Clearing your history prevents that history from being displayed in your Search History or chat history, but does not delete information from our search logs, which are retained and de-

identified as described above or as you have instructed through the privacy dashboard. If you are signed-in to a work or school Microsoft account using Microsoft Search in Bing, you can export your Microsoft Search in Bing search history, but you cannot delete it. Your Microsoft Search in Bing service administrator can see aggregated search history across all enterprise users but cannot see specific searches by user. However, if you are using Bing Chat for Enterprise while signed-in to a work or school Microsoft account, your Bing Chat for Enterprise conversations will not be saved or stored.

Third-party services that use Bing. You may access Bing-powered experiences when using third-party services, such as those from Yahoo!. In order to provide these services, Bing receives data from these and other partners, including your search query and related data (such as date, time, IP address, and a unique identifier). This data will be sent to Microsoft to provide the search service. Microsoft will use this data as described in this statement or as further limited by our contractual

obligations with our partners. You should refer to the privacy policies of the third-party services for any questions about how they collect and use data.

Data passed to destination website. When you select a search result or advertisement from a Bing search results page and go to the destination website, the destination website will receive the standard data your browser sends to every web site you visit—such as your IP address, browser type and language, and the host name of the site you came from (in this case, https://www.bing.com/).

Sharing data from Bing and Bing-powered experiences with third parties. We share some de-identified data (data where the identity of a specific person is not known) from Bing and Bing-powered experiences with selected third parties. Before we do so, we run the data through a process designed to remove certain sensitive data that users may have included in the search terms themselves (such as social security numbers or credit card numbers). Additionally, we require these third parties to

keep the data secure and to not use the data for purposes other than for which it is provided.

Cortana

Cortana is your personal productivity assistant in Microsoft 365. As a digital assistant, Cortana is designed to help you achieve more with less effort so you can focus on what matters and can answer a wide range of questions about things such as weather, sports, stocks, and general information. When you ask questions, the data Cortana collects depends on whether you are using the consumer or enterprise version.

This section applies to the consumer version of Cortana experiences in Windows 10 and Windows 11. If you are using Cortana with an account provided by an organization, such as a work or school account, see the Notice to end users section of this privacy statement. Learn more about the enterprise version of Cortana in Microsoft 365.

When you ask Cortana a question, whether you are speaking or typing, Cortana collects that question as a text string. To answer your questions Cortana uses the Bing service. For information about the data Bing collects, see the Bing section of this privacy statement.

By default, if you speak your question, Cortana also collects speech transcription data and does not collect voice clips. You have the option to provide your consent and allow Microsoft to collect voice clips. If you choose to opt in and allow Microsoft to collect voice clips, the voice clip files are stored and anonymized and will not be associated with your Microsoft account or any other Microsoft IDs. This anonymous data is used to improve the product. For more information about Microsoft and your voice data, see the Speech Recognition Technologies section of this privacy statement.

Cortana legacy. Cortana in Windows 10 version 1909 and earlier collects user query data (a text transcription of the question the user asked), which is anonymized and used for

product maintenance. Cortana in Windows 10 version 1909 also uses the Bing service to answer your questions. For information about the data Bing collects, see the Bing section of the Privacy Statement.

Learn more about Cortana and privacy.

Microsoft Edge

Whenever you use a web browser to access the internet, data about your device ("standard device data") is sent to the websites you visit and online services you use. Standard device data includes your device's IP address, browser type and language, access times, and referring website addresses. This data might be logged on those websites' or online services' web servers. Which data is logged and how that data is used depends on the privacy practices of the websites you visit and web services you use. Certain features in Microsoft Edge, such as when you open a new tab in the browser, connect you to Microsoft Start Content and your experiences with such content is covered by the Microsoft Start section of this privacy statement. Additionally,

Microsoft Edge sends a unique browser ID to certain websites to enable us to develop aggregate data used to improve browser features and services.

Microsoft Edge for Windows, Linux, and macOS. Microsoft Edge is the default web browser for Windows 10 and later and is also available on other supported versions of Windows and macOS.

Data about how you use your browser, such as your browsing history, web form data, temporary internet files, and cookies, is stored on your device. You can delete this data from your device using Clear Browsing History.

Microsoft Edge allows you to capture and save content on your device, such as:

- **Settings and More**. Allows you to manage your favorites, downloads, history, extensions, and collections.
- **Collections**. Allows you to collect text, images, videos, and other content in a note page in your browser. When you drag content into your collection, it is cached on

your device and can be deleted through your collection.
- **Website Pin to Taskbar**. Allows you to pin your favorite websites to the Windows taskbar. Websites will be able to see which of their webpages you have pinned, so they can provide you a notification badge letting you know there is something new for you to check out on their websites.

Microsoft collects data necessary to provide features you request in Microsoft Edge. When signed into Microsoft Edge using your Microsoft personal account or work or school account, Microsoft Edge will sync your browser data saved on your device across other signed-in devices. You may choose which browser data to sync, including your favorites, browsing history, extensions and associated data, settings, open tabs, autofill form entries (such as your name, address, and phone number), passwords, payment information, and other data types as they become available. If you choose to sync extensions that you acquired from third-party web stores, a copy of those extensions will be

downloaded directly from those web stores on your synced device(s). If you have turned on Password Monitor, your saved credentials are hashed, encrypted and sent to Microsoft's Password Monitor service to warn you if your credentials were detected as part of a malicious attack or a breach. Microsoft does not retain this data after the check is complete. You can disable or configure syncing in the Microsoft Edge settings.

When you sign into Microsoft Edge with your Microsoft personal account or work or school account, Microsoft Edge will store your account's privacy preferences. Microsoft Edge will use the stored preferences to migrate your account's privacy choices across your signed-in devices, including during Windows device set up or when you sign into Microsoft Edge with your account on a new device.

Microsoft Edge's **Search and site suggestions** uses your search queries and browsing history to provide you with faster browsing and more relevant search recommendations. Microsoft Edge sends the information you type into the

browser address bar to the default search provider configured in the address bar to offer search recommendations as you type each character. You can turn off these features at any time in the browser settings. In order to provide search results, Microsoft Edge sends your search queries, standard device information, and location (if you have location enabled) to your default search provider. If Bing is your default search provider, we use this data as described in the Bing section of this privacy statement.

Microsoft Edge collects and uses data from your search activity across the web, including websites Microsoft does not own or operate, to improve Microsoft services, such as Microsoft Edge, Microsoft Bing and Microsoft News. This data may include the search query, the search results that are displayed to you, demographic information that is part of the search results, and the interaction you have with those search results, such as the links you click. Microsoft Edge takes steps to de-identify the data it collects by removing data that identifies the person or device from which it

was collected and retains this data for one year from when it is collected. Microsoft does not use this collected data to personalize or provide ads to you. You can turn off the collection of this data at any time in the browser settings.

Microsoft Edge downloads content from Microsoft services to enhance your browsing experiences; for example, when data is downloaded to prerender site content for faster browsing or to provide content required to power features you choose to use, such as providing templates for Collections.

You may also choose to share your Microsoft Edge browsing activity to allow us to personalize Microsoft Edge and Microsoft services like ads, search, shopping, and news. Microsoft Edge browsing activity includes your history, favorites, usage data, web content, and other browsing data. For more information about our **advertising privacy policies** see the Advertising section of the privacy statement. In the Microsoft privacy dashboard you can control the use of your browsing activity for

personalized ads in the **See ads that interest you** setting. If you disable this setting in the Microsoft privacy dashboard you will continue to receive personalized web experiences like search and news based on your browsing activity. You may stop sharing your Microsoft Edge browsing activity by disabling **Allow Microsoft to use your browsing activity including history, favorites, usage and other browsing data to personalize Microsoft Edge and Microsoft services like ads, search, shopping and news** within Edge settings. When using Bing chat features in the Microsoft Edge sidebar, you can choose to allow Bing to access the content of the webpage you are viewing in order to provide further insights, such as page summaries. Use of data connected with Bing conversational experiences is described in the Bing section of this privacy statement.

Microsoft Edge collects required diagnostic data to solve problems and to keep Microsoft Edge up to date, secure, and operating properly. Required diagnostic data also helps us improve Microsoft Edge and Windows.

Separate from your search activity data mentioned above, you can choose to send optional diagnostic data about how you use Microsoft Edge and information about your browser activity, including browsing history and search terms to Microsoft to help us improve Microsoft Edge and other Microsoft products and services. For Microsoft Edge on Windows 10 and later, this information is provided when you have enabled optional diagnostic data. For details, see the Windows Diagnostics section of the privacy statement. For Microsoft Edge on other operating systems, optional diagnostic information is provided when you enable **Improve Microsoft products by sending data about how you use the browser** or **Make searches and Microsoft products better by sending info about websites you visit in Microsoft Edge** in the browser settings.

The diagnostic data collected by Microsoft Edge is transmitted to Microsoft and is stored with one or more unique identifiers that help us recognize an individual browser installation

on a device and understand the browser's service issues and use patterns.

Learn more about Microsoft Edge, browsing data, and privacy.

Microsoft Edge on iOS and Android. Microsoft Edge on iOS and Android devices collects data necessary to provide features you request in Microsoft Edge. Microsoft also collects required diagnostic data to solve problems and to keep Microsoft Edge up to date, secure, and operating properly. Required diagnostic data also helps us improve Microsoft Edge.

Additionally, you may share optional diagnostic data about how you use Microsoft Edge and information about websites you visit (browsing history) for personalized experiences on your browser, Windows, and other Microsoft products and services. This information also helps us improve Microsoft Edge and other Microsoft products and services. This optional diagnostic data is sent to us when you enable **Share usage data for personalization** or **Share info about websites you visit** in the browser settings.

The diagnostic data collected by Microsoft Edge is transmitted to Microsoft and is stored with one or more unique identifiers that help us recognize an individual user on a device and understand the browser's service issues and use patterns.

Microsoft Edge uses data from your search activity across the web, including search activity on websites Microsoft does not own or operate, to improve Microsoft services like Microsoft Edge, Microsoft Bing, and Microsoft News. The data Microsoft Edge collects may include personal data; however, Microsoft Edge takes steps to scrub and de-identify the data. Microsoft Edge does not use this data to personalize or provide ads for you. You can turn off the collection of this data at any time in the browser settings. Learn more about Search results data for product improvement.

For information about the privacy practices of legacy versions Microsoft Edge (versions 44 and below), see the Web browsers—Microsoft Edge Legacy and Internet Explorer section of the privacy statement.

Microsoft Translator

Microsoft Translator is a machine translation system and service designed to automatically translate text and voice input between numerous supported languages. Microsoft Translator is made available as a stand-alone consumer app for Android, iOS, and Windows and its service capabilities are also integrated in a variety of Microsoft products and services, such as Translator Hub, Translator for Bing, and Translator for Microsoft Edge. Microsoft Translator processes the text, image, and voice data you submit, as well as device and usage data. We use this data to provide Microsoft Translator, personalize your experiences, and improve our products and services. Microsoft has implemented business and technical measures designed to help de-identify the data you submit to Microsoft Translator. For example, when we randomly sample text and audio to improve Microsoft Translator and Microsoft’s speech recognition technologies, we delete identifiers and certain text, such as email addresses and some

number sequences, detected in the sample that could contain personal data. To learn more about how Microsoft manages your voice data, see Speech recognition technologies.

Separate from Microsoft Translator, Microsoft translation services are available as features in other Microsoft products and services that have different privacy practices than Microsoft Translator. For more information on the Microsoft Azure Cognitive Services Translator Text API, Custom Translator, and Translator Speech API, see the Enterprise and developer products section of this privacy statement. For the Translate feature in Microsoft 365 apps and Skype, see the Productivity and communications products section of this privacy statement.

SwiftKey

The Microsoft Swiftkey keyboard and related cloud-based services (collectively, the "SwiftKey Services") process data about words you use and how you type and use this data to learn your writing style and provide

personalized autocorrection and predictive text that adapts to you. We also use this data to offer a range of other features, such as hashtag and emoji predictions.

SwiftKey prediction technology learns from the way you use language to build a personalized language model. This model is an optimized view of the words and phrases that you use most often in context and reflects your unique writing style. The model itself contains the words you commonly type arranged in a way that enables SwiftKey's algorithms to make predictions, based on text you have already entered. The model draws from all scenarios in which you use your keyboard, including when you type while using apps or visiting websites. The SwiftKey keyboard and model attempt to avoid collecting sensitive data, by not collecting data from certain fields such as those recognized as containing password or payment data. SwiftKey Services do not log, store, or learn from data you type, or the data contained in your model, unless you choose to share your data with us (as described further below). When you use SwiftKey Services, we

also collect device and usage data. We use de-identified device and usage data to analyze service performance and help improve our products.

The SwiftKey Services also include an optional cloud component called a SwiftKey Account. If you choose to create a SwiftKey Account, your language model will be synced with the SwiftKey Account cloud service, so you can benefit from that model on the different devices you use and access additional services such as prediction synchronization and backup. When you create a SwiftKey Account, Microsoft will also collect your email address and basic demographic data. All data collected is transferred to our servers over encrypted channels.

You may also opt in to share your language, typing data, and/or voice clips for the purposes of improving Microsoft products and services. Depending on the opt-ins you choose, SwiftKey may send short snippets of data about what and how you type and/or your voice clips, and related correction data to our

servers for processing. These text snippets and/or voice clips are used in various automated processes to validate that our prediction services are working correctly and to make product improvements. To preserve your privacy, SwiftKey Services de-identify these text snippets, and even if you have a SwiftKey Account, these text snippets and/or voice clips will not be linked to it. To learn more about how Microsoft manages your voice data, see Speech recognition technologies.

If you sign into your SwiftKey Account and opt to share your language and typing data or voice clips, Microsoft will process your shared data in order to look for new patterns of language usage across our user base. This allows us to improve our basic models for individual languages. Language and typing data used in this process is aggregated and any words or combinations of words that might be personal to individuals or small groups of users are filtered out.

You can withdraw your consent to share your language and typing data or voice clips for product improvement at any time in SwiftKey Settings. You can also withdraw your consent for SwiftKey Services to retain your personal data in SwiftKey Settings. When you withdraw consent for SwiftKey to retain your personal data, all personal data collected through your use of the SwiftKey Services will be deleted.

You may receive occasional notifications on your device alerting you to product updates and features that may be of interest to you. You can disable these notifications at any time in the SwiftKey Settings.

Windows

Windows is a personalized computing environment that enables you to seamlessly roam and access services, preferences, and content across your computing devices from phones to tablets to the Surface Hub. Rather than residing as a static software program on your device, key components of Windows are cloud-based, and both cloud and local elements of Windows are updated regularly, providing you with the latest

improvements and features. In order to provide this computing experience, we collect data about you, your device, and the way you use Windows. And because Windows is personal to you, we give you choices about the personal data we collect and how we use it. Note that if your Windows device is managed by your organization (such as your employer or school), your organization may use centralized management tools provided by Microsoft or others to access and process your data and to control device settings (including privacy settings), device policies, software updates, data collection by us or the organization, or other aspects of your device. Additionally, your organization may use management tools provided by Microsoft or others to access and process your data from that device, including your interaction data, diagnostic data, and the contents of your communications and files. For more information about data collection in Windows, see Data collection summary for Windows. This statement discusses Windows 10 and Windows 11 and references to Windows in this section relate to those product versions. Earlier versions of Windows (including Windows Vista, Windows 7,

Windows 8, and Windows 8.1) are subject to their own privacy statements.

Activation

When you activate Windows, a specific product key is associated with the device on which your software is installed. The product key and data about the software and your device is sent to Microsoft to help validate your license to the software. This data may be sent again if there is a need to re-activate or validate your license. On phones running Windows, device and network identifiers, as well as device location at the time of the first power-up of the device, are also sent to Microsoft for the purpose of warranty registration, stock replenishment, and fraud prevention.

Activity history

Activity history helps keep track of the things you do on your device, such as the apps and services you use, the files you open, and the websites you browse. Your activity history is created when using different apps and

features such as Microsoft Edge Legacy, some Microsoft Store apps, and Microsoft 365 apps and is stored locally on your device. If you've signed in to your device with a work or school account and give your permission, Windows sends your activity history to Microsoft. Once your activity history is in the cloud, Microsoft uses that data to enable cross-device experiences, to provide you with the ability to continue those activities on other devices, to provide personalized experiences (such as ordering your activities based on duration of use) and relevant suggestions (such as anticipating what your needs might be based on your activity history), and to help improve Microsoft products.

You can turn settings off or on for sending your activity history to Microsoft and storing activity history locally on your device, and you can also clear your device's activity history at any time by going to **Privacy > Activity history** in the Windows settings app. Learn more about activity history in Windows.

Advertising ID

Windows generates a unique advertising ID for each person using a device, which app developers and advertising networks can then use for their own purposes, including providing relevant advertising in apps. When the advertising ID is enabled, both Microsoft apps and third-party apps can access and use the advertising ID in much the same way that websites can access and use a unique identifier stored in a cookie. Thus, your advertising ID can be used by app developers and advertising networks to provide more relevant advertising and other personalized experiences across their apps and on the web. Microsoft collects the advertising ID for the uses described here only when you choose to enable the advertising ID as part of your privacy setting.

The advertising ID setting applies to Windows apps using the Windows advertising identifier. You can turn off access to this identifier at any time by turning off the advertising ID in the Windows settings app. If you choose to turn it on again, the advertising ID will be reset and a new identifier will be generated. When a third-

party app accesses the advertising ID, its use of the advertising ID will be subject to its own privacy policy. Learn more about advertising ID in Windows.

The advertising ID setting does not apply to other methods of interest-based advertising delivered by Microsoft or third parties, such as cookies used to provide interest-based display ads on websites. Third-party products accessed through or installed on Windows may also deliver other forms of interest-based advertising subject to their own privacy policies. Microsoft delivers other forms of interest-based ads in certain Microsoft products, both directly and by partnering with third-party ad providers. For more information on how Microsoft uses data for advertising, see the How we use personal data section of this statement.

Diagnostics

Microsoft collects Windows diagnostic data to solve problems and to keep Windows up to date, secure, and operating properly. It also helps us improve Windows and related

Microsoft products and services and, for customers who have turned on the “Tailored experiences” setting, to provide more relevant tips and recommendations to tailor Microsoft and third-party products and services for Windows to the customer’s needs. This data is transmitted to Microsoft and stored with one or more unique identifiers that can help us recognize an individual user on an individual device and understand the device's service issues and use patterns.

There are two levels of diagnostic and activity data: Required diagnostic data and Optional diagnostic data. Certain product documentation and other materials refer to Required diagnostic data as Basic diagnostic data and to Optional diagnostic data as Full diagnostic data.

If an organization (such as your employer or school) uses Azure Active Directory (AAD) to manage the account it provides to you and enrolls your device in the Windows diagnostic data processor configuration, Microsoft’s processing of diagnostic data in connection

with Windows is governed by a contract between Microsoft and the organization. If an organization uses Microsoft management tools or engages Microsoft to manage your device, Microsoft and the organization will use and process diagnostic and error data from your device to allow the management, monitoring, and troubleshooting of your devices managed by the organization, and for other purposes of the organization.

Required diagnostic data includes information about your device, its settings and capabilities, and whether it is performing properly. We collect the following Required diagnostic data:

- Device, connectivity, and configuration data:
  - Data about the device such as the processor type, OEM manufacturer, type of battery and capacity, number and type of cameras, firmware, and memory attributes.
  - Network capabilities and connection data such as the device's IP address, mobile network (including IMEI and

mobile operator), and whether the device is connected to a free or paid network.
    - Data about the operating system and its configuration such as the OS version and build number, region and language settings, diagnostics data settings, and whether the device is part of the Windows Insider program.
    - Data about connected peripherals such as model, manufacturer, drivers, and compatibility data.
    - Data about the applications installed on the device such as application name, version, and publisher.
- Whether a device is ready for an update and whether there are factors that may impede the ability to receive updates, such as low battery, limited disk space, or connectivity through a paid network.
- Whether updates complete successfully or fail.
- Data about the reliability of the diagnostics collection system itself.
- Basic error reporting, which is health data about the operating system and

applications running on your device. For example, basic error reporting tells us if an application, such as Microsoft Paint or a third-party game, hangs or crashes.

Optional diagnostic data includes more detailed information about your device and its settings, capabilities, and device health. Optional diagnostic data also includes data about the websites you browse, device activity (also sometimes referred to as usage), and enhanced error reporting that helps Microsoft to fix and improve products and services for all users. When you choose to send Optional diagnostic data, Required diagnostic data will always be included, and we collect the following additional information:

- Additional data about the device, connectivity, and configuration, beyond that collected under Required diagnostic data.
- Status and logging information about the health of operating system and other system components beyond that collected about the update and diagnostics systems under Required diagnostic data.

- App activity, such as which programs are launched on a device, how long they run, and how quickly they respond to input.
- Browser activity, including browsing history and search terms, in Microsoft browsers (Microsoft Edge or Internet Explorer).
- Enhanced error reporting, including the memory state of the device when a system or app crash occurs (which may unintentionally contain user content, such as parts of a file you were using when the problem occurred). Crash data is never used for Tailored experiences as described below.

Some of the data described above may not be collected from your device even if you choose to send Optional diagnostic data. Microsoft minimizes the volume of Optional diagnostic data it collects from all devices by collecting some of the data from only a subset of devices (sample). By running the Diagnostic Data Viewer tool, you can see an icon which indicates whether your device is part of a sample and also which specific data is collected from your device. Instructions for

how to download the Diagnostic Data Viewer tool can be found in the Windows settings app under Diagnostics & feedback.

Specific data items collected in Windows diagnostics are subject to change to give Microsoft flexibility to collect the data needed for the purposes described. For example, to enable Microsoft to troubleshoot the latest performance issue impacting users' computing experience or update a Windows device that is new to the market, Microsoft may need to collect data items that were not collected previously. For a current list of data types collected at **Required diagnostic data** and **Optional diagnostic data**, see Windows Required (Basic level) diagnostic events and fields or Windows Optional (Full level) diagnostic data. We provide limited portions of error report information to partners (such as the device manufacturer) to help them troubleshoot products and services which work with Windows and other Microsoft product and services. They are only permitted to use this information to repair or improve those products and services. We may also

share some aggregated, de-identified diagnostic data, such as general usage trends for Windows apps and features, with selected third parties. Learn more about diagnostic data in Windows.

Inking and typing Recognition. You also can choose to help Microsoft improve inking and typing recognition by sending inking and typing diagnostic data. If you choose to do so, Microsoft will collect samples of the content you type or write to improve features such as handwriting recognition, autocompletion, next word prediction, and spelling correction in the many languages used by Microsoft customers. When Microsoft collects inking and typing diagnostic data, it is divided into small samples and processed to remove unique identifiers, sequencing information, and other data (such as email addresses and numeric values) which could be used to reconstruct the original content or associate the input to you. It also includes associated performance data, such as changes you manually make to text, as well as words you've added to the

dictionary. Learn more about improving inking and typing in Windows.

If you choose to turn on **Tailored experiences**, we will use your Windows diagnostic data (Required or Optional as you have selected) to offer you personalized tips, ads, and recommendations to enhance Microsoft experiences. If you have selected Required as your diagnostic data setting, personalization is based on information about your device, its settings and capabilities, and whether it is performing properly. If you have selected Optional, personalization is also based on information about how you use apps and features, plus additional information about the health of your device. However, we do not use information about the websites you browse, the content of crash dumps, speech, typing, or inking input data for personalization when we receive such data from customers who have selected Optional.

Tailored experiences include suggestions on how to customize and optimize Windows, as well as ads and recommendations for

Microsoft and third-party products and services, features, apps, and hardware for your Windows experiences. For example, to help you get the most out of your device, we may tell you about features you may not know about or that are new. If you are having a problem with your Windows device, you may be offered a solution. You may be offered a chance to customize your lock screen with pictures, or to be shown more pictures of the kind you like, or fewer of the ones you do not. If you stream movies in your browser, you may be recommended an app from the Microsoft Store that streams more efficiently. Or, if you are running out of space on your hard drive, Windows may recommend you try OneDrive or purchase hardware to gain more space. Learn more about tailored experiences in Windows.

Feedback Hub

Feedback Hub is a preinstalled app that provides a way to gather feedback on Microsoft products and installed first party and third-party apps. You can sign into Feedback Hub using either your personal

Microsoft account or an account provided by your organization (such as your employer or school) that you use to sign into Microsoft products. Signing in with your work or school account allows you to submit feedback to Microsoft in association with your organization.

Any feedback you provide whether using your work or school account or personal Microsoft account may be publicly viewable depending on the settings configured by your organization's administrators. Additionally, if feedback is provided using your work or school account, your feedback can be viewed through the Feedback Hub by your organization's administrators.

When you submit feedback to Microsoft about a problem or add more details to a problem, diagnostic data will be sent to Microsoft to improve Microsoft products and services. Depending on your Diagnostic data settings in the **Diagnostics & feedback** section of the Windows settings app, Feedback Hub will either send diagnostic data automatically or

you will have the option to send it to Microsoft at the time you provide feedback. Based on the category chosen when submitting feedback, there may be additional personal data collected that helps to further troubleshoot issues; for example, location related information when submitting feedback about location services or gaze related information when submitting feedback on Mixed Reality. Microsoft may also share your feedback along with the data collected when you submit your feedback with Microsoft partners (such as a device manufacturer, or firmware developer) to help them troubleshoot products and services that work with Windows and other Microsoft products and services. Learn more about diagnostic data in Windows.

Location services and recording

Windows location service. Microsoft operates a location service that helps determine the precise geographic location of a specific Windows device. Depending on the capabilities of the device, the device's location can be determined with varying degrees of

accuracy and may in some cases be determined precisely. When you have enabled location on a Windows device, or you have given permission for Microsoft apps to access location information on non-Windows devices, data about cell towers and Wi-Fi access points and their locations is collected by Microsoft and added to the location database after removing any data identifying the person or device from which it was collected. This de-identified location information is used to improve Microsoft's location services and, in some instances, shared with our location service provider partners, currently HERE (see https://www.here.com/) and Skyhook (see https://www.skyhook.com) to improve the location services of the provider.

Windows services and features, apps running on Windows, and websites opened in Windows browsers can access the device's location through Windows if your settings allow them to do so. Some features and apps request location permission when you first install Windows, some ask the first time you use the app, and others ask every time you access the

device’s location. For information about certain Windows apps that use the device’s location, see the Windows apps section of this privacy statement.

When an app or feature accesses the device’s location and you are signed in with a Microsoft account, your Windows device will also upload its location to the cloud where it is available across your devices to other apps or services that use your Microsoft account and for which you’ve granted permission. We will retain only the last known location (each new location replaces the previous one). Data about a Windows device's recent location history is also stored on the device even if not using a Microsoft account, and certain apps and Windows features can access this location history. You can clear your device's location history at any time in the Windows settings app.

In the Windows settings app, you can also view which apps have access to the device’s precise location or your device's location history, turn off or on access to the device’s

location for particular apps, or turn off access to the device's location. You can also set a default location, which will be used when the location service can't detect a more exact location for your device.

There are some exceptions to how your device's location can be determined that are not directly managed by the location settings.

Desktop apps are a specific type of app that won't ask for separate permission to discover your device location information and won't appear in the list that allows you to choose apps that can use your location. They can be downloaded from the Microsoft Store, downloaded from the internet, or installed with some type of media (such as a CD, DVD, or USB storage device). They're opened using an .EXE, .MSI, or .DLL file, and they typically run on your device, unlike web-based apps (which run in the cloud). Learn more about third-party desktop apps and how they may still be able to determine your device's location when the device's location setting is off.

Some web-based experiences or third-party apps that surface on Windows could use other technologies (such as Bluetooth, Wi-Fi, cellular modem, etc.) or cloud-based location services to determine your device's location with varying degrees of accuracy even when you've turned off the device location setting.

In addition, to facilitate getting help in an emergency, whenever you make an emergency call, Windows will attempt to determine and share your precise location, regardless of your location settings. If your device has a SIM card or is otherwise using cellular service, your mobile operator will have access to your device's location. Learn more about location in Windows.

General Location. If you turn on Location services, apps that cannot use your precise location may still have access to your general location, such as your city, postal code, or region.

Find my device. The Find my device feature allows an administrator of a Windows device to find the location of that device from

account.microsoft.com/devices. To enable Find my device, an administrator needs to be signed in with a Microsoft account and have the location setting enabled. This feature will work even if other users have denied access to location for all their apps. When the administrator attempts to locate the device, users will see a notification in the notification area. Learn more about Find my device in Windows.

Recording. Some Windows devices have a recording feature that allows you to capture audio and video clips of your activity on the device, including your communications with others. If you choose to record a session, the recording will be saved locally on your device. In some cases, you may have the option to transmit the recording to a Microsoft product or service that broadcasts the recording publicly. **Important: You should understand your legal responsibilities before recording and/or transmitting any communication. This may include obtaining the prior consent of everyone participating in the conversation or any other authorizations as required.**

Microsoft is not responsible for how you use recording features or your recordings.

Phone Link - Link to Windows

Phone Link - Link to Windows The Phone Link app lets you link your Android phone with your Microsoft Account, enabling a variety of cross-device experiences. You can use Phone Link to see recent photos from your Android phone on your Windows device; make and receive calls from your Android phone on your Windows device; view and send text messages from your Windows device; view, dismiss, or perform other actions to your Android phone notifications from your Windows device; share your phone screen on your Windows device through Phone Link’s mirroring function; and instantly access Android apps installed on your Android phone on your Windows device.

To use Phone Link, the Phone Link app must be installed on your Windows device and the Link to Windows app must be installed on your Android phone.

To use Phone Link, you must log into your Microsoft account on the Phone Link app on your Windows device and on the Link to Windows app on your Android phone. Your Android phone and your Windows device must be connected to the internet. Some features will require you to enable Bluetooth and pair your phone with your PC. To use the Calls feature, your Android phone must also have Bluetooth enabled.

During setting up your Windows device, you can choose to link your phone with your Microsoft account. This is done by signing into Link to Windows on your Android phone, granting permissions and completing the onboarding experience. Once complete, Link to Windows will sync your data, such as your text messages, contacts, call history, photos, notifications, and other information, to all your Windows PCs where you have signed into your Microsoft account. See below for details on how your data is used.

As part of providing Phone Link’s features to you, Microsoft collects performance, usage,

and device data that includes, for example, the hardware capabilities of your mobile phone and Windows device, the number and duration of your sessions on Phone Link, and the amount of time you spent during setup.

You can unlink your Android phone from your Windows device at any time by going into your Phone Link app settings and choosing to remove your Android phone. You can do the same from the app settings on the Link to Windows app on your Android phone. For detailed information, see our support page.

Text Messages. Phone Link allows you to view text messages delivered to your Android phone on your Windows device and send text messages from your Windows device. Only text messages received and sent within the last 30 days are visible on your Windows device. These text messages are temporarily stored on your Windows device. We never store your text messages on our servers or change or delete any text messages on your Android phone. You can see messages sent via SMS (Short Message Service) and MMS

(Multimedia Messaging Service) on Android devices, and messages sent via RCS (Rich Communication Services) on select Samsung devices on select mobile operator networks. To provide this functionality, Phone Link accesses the content of your text messages and the contact information of the individuals or businesses from whom you are receiving or sending text messages.

Calls. Phone Link allows you to make and receive calls from your Android phone on your Windows device. Through Phone Link, you can also view your recent calls on your Windows device. To activate this feature, you must enable certain permissions on both your Windows device and Android phone, such as call logs access and permission to make phone calls from your PC. These permissions can be revoked at any time under the Phone Link Settings page on your Windows device and your Android phone's settings. Only calls received and dialed within the last 30 days are visible under call logs on your Windows device. These call details are temporarily stored on

your Windows device. We do not change or delete your call history on your Android phone.

Photos. Phone Link allows you to copy, share, edit, save, or delete photos from your Android phone on your Windows device. Only a limited number of your most recent photos from the Camera Roll and Screenshots folders on your Android phone will be visible on your Windows device at any given time. These photos are temporarily stored on your Windows device and as you take more photos on your Android phone, we remove the temporary copies of the older photos from your Windows device. We never store your photos on our servers or change or delete any photos on your Android phone.

Notifications. Phone Link allows you to view your Android phone's notifications on your Windows device. Through Phone Link, you can read and dismiss your Android phone's notifications from your Windows device or perform other actions related to the notifications. To activate this Phone Link feature, you must enable certain permissions,

such as sync notifications, on both your Windows device and Android phone. These permissions can be revoked at any time under the Phone Link Settings page on your Windows device and your Android phone's settings. For detailed information, see our support page.

Phone Screen Mirroring. On supported devices, Phone Link allows you to view your Android phone's screen on your Windows device. Your Android phone screen will be visible on your Windows device as a pixel stream and any audio that you enable on your Android phone screen while it is linked to your Windows device through Phone Link will play through your Android phone.

Apps mirroring. On supported devices, Phone Link allows you to use your Android apps that are installed on your Android phone on your Windows device. For example, you can launch a music app in your Windows session and listen to audio from that app on your PC speakers. Microsoft collects a list of your installed Android apps and recent activity to provide the service and show you your most

recently used apps. Microsoft does not store what apps you have installed or any of the information displayed by the app in your experience with it.

Content transfer. On supported devices, Phone Link allows you to copy and paste contents such as files, documents, photos, etc. between your Android phone and your Windows device. You can transfer content from your Android phone to your Windows device and from your Windows device to your Android phone by drag and drop contents between the devices.

Instant Hotspot. On supported devices, Link to Windows enables users to share mobile hotspot information with their paired PC over secure Bluetooth communication. Your PC application can then be connected to the internet through the Windows network flyout. Please note mobile data charges may apply depending on the mobile data plan you have.

Contacts sync. Link to Windows allows you to sync your Android contacts into the Microsoft cloud to access them in other Microsoft products and services. You can enable this

feature by going into Link to Windows settings and enabling “Contacts sync” feature. Your contacts information is stored online and associated with your Microsoft account. You may choose to disable sync and delete these contacts at any time. Learn more.

Text-to-voice. Phone Link features include accessibility functionality such as text-to-voice. You can activate a text-to-voice feature, which allows you to hear the contents of a text message or notification as audio. If you activate this feature, your text messages and notifications will be read out loud as they are received.

Office Enterprise. Link to Windows allows you to insert photos into PowerPoint Online and Word Online directly from your mobile phone. This requires your IT Administrator to have enabled Optional Connected Experiences for Microsoft Office applications and you will need to associate your mobile device with your Azure Active Directory (AAD) account and provide Photos permission to your account. After onboarding, your session will last 15

minutes to enable you to transfer your Photos from your mobile device. In order to use this feature again, you will need to scan your QR code again. Link to Windows does not collect your AAD account or information about your Enterprise. In order to provide this service, Microsoft uses a cloud service to relay your files for the purpose of inserting the photos into your PowerPoint Online or Word Online files.

Security and safety features

Device encryption. Device encryption helps protect the data stored on your device by encrypting it using BitLocker Drive Encryption technology. When device encryption is on, Windows automatically encrypts the drive Windows is installed on and generates a recovery key. The BitLocker recovery key for your personal device is automatically backed up online in your personal Microsoft OneDrive account. Microsoft doesn't use your individual recovery keys for any purpose.

Malicious Software Removal Tool. The Malicious Software Removal Tool (MSRT) runs

on your device at least once per month as part of Windows Update. MSRT checks devices for infections by specific, prevalent malicious software ("malware") and helps remove any infections found. When the MSRT runs, it will remove the malware listed on the Microsoft Support website if the malware is on your device. During a malware check, a report will be sent to Microsoft with specific data about malware detected, errors, and other data about your device. If you do not want MSRT to send this data to Microsoft, you can disable MSRT's reporting component.

Microsoft Family. Parents can use Microsoft Family Safety to understand and set boundaries on how their child is using their device. Please carefully review the information at Microsoft Family Safety if choosing to create or join a family group. If you live in a region that requires permission to create an account to access Microsoft services, you may be prompted to request or give parental consent. If a user is under the statutory age in your region, during the registration process they will be prompted to request consent from

a parent or guardian by entering an adult's email. When Family activity reporting is turned on for a child, Microsoft will collect details about how the child uses their device and provide parents with reports of that child's activities. Activity reports are routinely deleted from Microsoft servers.

Microsoft Defender SmartScreen and Smart App Control. Microsoft strives to help protect your device and passwords from unsafe apps, files, and web content.

Microsoft Defender SmartScreen helps protect you when using our services by identifying threats to you, your device, and your passwords. These threats might include potentially unsafe apps or web content that Microsoft Defender SmartScreen discovers while checking websites you visit, files you download, and apps you install and run. When Microsoft Defender SmartScreen checks web and app content, data about the content and your device is sent to Microsoft, including the full web address of the content. When additional analysis is needed to identify

security threats, information about the suspicious website or app—such as content displayed, sounds played, and application memory—may be sent to Microsoft. This data will only be used for security purposes in detecting, protecting against, and responding to security incidents, identity theft, fraud, or other malicious, deceptive, or illegal activities. If Microsoft Defender SmartScreen detects that content is potentially unsafe, you will see a warning in place of the content. Microsoft Defender SmartScreen can be turned on or off in the Windows Security app.

Where supported, Smart App Control helps check software that is installed and runs on your device to determine if it is malicious, potentially unwanted, or poses other threats to you and your device. On a supported device, Smart App Control starts in evaluation mode and the data we collect for Microsoft Defender SmartScreen such as file name, a hash of the file's contents, the download location, and the file's digital certificates, is used to help determine whether your device is a good candidate to use Smart App Control for

additional security protection. Smart App Control is not enabled and will not block during evaluation mode. Some devices may not be good candidates if Smart App Control would otherwise get in the way and interfere with a user's otherwise intended and legitimate tasks – for instance, developers who use a lot of unsigned files. If you are a good candidate for Smart App Control, then it will automatically be turned on, and will provide additional protection to your device beyond Microsoft Defender SmartScreen. Otherwise, Smart App Control will be unavailable and permanently turned off. If your device is unsupported or not a good candidate for Smart App Control, Microsoft Defender SmartScreen will continue to help protect your device. When Smart App Control is enabled and identifies an app as malicious, potentially unwanted, or unknown and unsigned, it will block and notify you prior to opening, running, or installing the app. Learn more about Smart App Control.

When either Microsoft Defender SmartScreen or Smart App Control checks a file, data about that file is sent to Microsoft, including the file

name, a hash of the file's contents, the download location, and the file's digital certificates.

Smart App Control can be turned on or off in the Windows Security app.

Microsoft Defender Antivirus. Microsoft Defender Antivirus looks for malware and other unwanted software, potentially unwanted apps, and other malicious content on your device. Microsoft Defender Antivirus is automatically turned on to help protect your device if no other antimalware software is actively protecting your device. If Microsoft Defender Antivirus is turned on, it will monitor the security status of your device. When Microsoft Defender Antivirus is turned on, or is running because Limited Periodic Scanning is enabled, it will automatically send reports to Microsoft that contain data about suspected malware and other unwanted software, potentially unwanted apps, and other malicious content, and it may also send files that could contain malicious content, such as malware or unknown files for further

inspection. If a report is likely to contain personal data, the report is not sent automatically, and you'll be prompted before it is sent. You can configure Microsoft Defender Antivirus not to send reports and suspected malware to Microsoft.

Speech, Voice Activation, Inking, and Typing

Speech. Microsoft provides both a device-based speech recognition feature and cloud-based (online) speech recognition technologies.

Turning on the Online speech recognition setting lets apps use Microsoft cloud-based speech recognition. Additionally, in Windows 10, the Online speech recognition setting enables your ability to use dictation within Windows.

Turning on speech while setting up a HoloLens device or installing Windows Mixed Reality allows you to use your voice for commands, dictation, and app interactions. Both device-based speech recognition and online speech

recognition settings will be enabled. With both settings enabled, while your headset is turned on the device will always be listening to your voice input and will send your voice data to Microsoft's cloud-based speech recognition technologies.

When you use cloud-based speech recognition technologies from Microsoft, whether enabled by the Online speech recognition setting or when you interact with HoloLens or voice typing, Microsoft collects and uses your voice recordings to provide the speech recognition service by creating a text transcription of the spoken words in the voice data. Microsoft will not store, sample, or listen to your voice recordings without your permission. To learn more about how Microsoft manages your voice data, see Speech recognition technologies.

You can use device-based speech recognition without sending your voice data to Microsoft. However, Microsoft cloud-based speech recognition technologies provide more accurate recognition than the device-based

speech recognition. When the online speech recognition setting is turned off, speech services that do not rely on the cloud and only use device-based recognition—like the live captions app, the Narrator app or the Windows Speech Recognition app—will still work and Microsoft won't collect any voice data.

You can turn off online speech recognition at any time. This will stop any apps that rely on the Online speech recognition setting from sending your voice data to Microsoft. If you are using a HoloLens or Windows Mixed Reality headset, you can also turn off device-based speech recognition at any time. This will stop the device from listening for your voice input. Learn more about speech recognition in Windows.

Voice Activation. Windows provides supported apps with the ability to respond and take action based on voice keywords that are specific to that app—for example allowing Cortana to listen and respond when you say "Cortana."

If you've given permission for an app to listen for voice keywords, Windows will be actively listening to the microphone for these keywords. Once a keyword is recognized, the app will have access to your voice recording, can process the recording, take action, and respond, such as with a spoken answer. The app may send the voice recording to its own services in the cloud to process the commands. Each app should ask you for permission before accessing voice recordings.

Additionally, voice activation can be enabled when the device is locked. If enabled, the relevant app will continue listening to the microphone for voice keywords when you have locked your device and can activate for anyone who speaks near the device. When the device is locked, the app will have access to the same set of capabilities and information as when the device is unlocked.

You can turn off voice activation at any time. Learn more about voice activation in Windows.

Even when you've turned off voice activation, some third-party desktop apps and services

could still be listening to the microphone and collect your voice input. Learn more about third-party desktop apps and how they may still be able to access your microphone even with these settings turned off.

Voice typing. In Windows 11, dictation has been updated and renamed as voice typing. Voice typing may use both device-based and online speech recognition technologies to power its speech-to-text transcription service. You can also choose to contribute voice clips to help improve voice typing. If you choose not to contribute voice clips, you can still use voice typing. You can change your selection anytime in the voice typing settings. Microsoft will not store, sample, or listen to your voice recordings without your permission. Learn more about Microsoft and your voice data.

Voice access. Windows enables everyone, including people with mobility disabilities, to control their PC and author text using their voice. For example, voice access supports scenarios like opening and switching between apps, browsing the web, and reading and

authoring mail. Voice access leverages modern, on-device speech recognition to accurately recognize speech and is supported without an internet connection. Learn more about voice access.

Inking & Typing Personalization. Your typed and handwritten words are collected to provide you with a custom word list, better character recognition to help you type and write on your device, and text suggestions that appear as you type or write.

You can turn off inking & typing personalization at any time. This will delete your customer word list stored on your device. If you turn it back on, you'll need to recreate your custom word list. Learn more about inking & typing personalization in Windows.

Sync and backup settings

When you sign into Windows with your Microsoft account or work or school account, Windows can store your settings, files, and device configuration data in Microsoft's servers. Windows will only use the stored

settings, files, and device configuration data to make it easier for you to migrate your experience on a different device.

You can turn off this feature and stop Windows from storing your settings, files, and configuration data from the Windows settings app. You can also delete the sync and backup data Windows has stored in the settings app.

Learn more about Windows backup and sync settings.

Update Services

Update Services for Windows includes Windows Update and Microsoft Update. Windows Update is a service that provides you with software updates for Windows software and other supporting software, such as drivers and firmware supplied by device manufacturers. Microsoft Update is a service that provides you with software updates for other Microsoft software such as Microsoft 365.

Windows Update automatically downloads Windows software updates to your device. You

can configure Windows Update to automatically install these updates as they become available (recommended) or have Windows notify you when a restart is required to finish installing updates. Apps available through the Microsoft Store are automatically updated through the Microsoft Store, as described in the Microsoft Store section of this privacy statement.

Web browsers—Microsoft Edge Legacy and Internet Explorer

This section applies to legacy versions of Microsoft Edge (versions 44 and below). See the Microsoft Edge section of the Privacy Statement for information about non-legacy versions of Microsoft Edge.

Microsoft Edge is the default web browser for Windows. Internet Explorer, the legacy browser from Microsoft, is also available in Windows. Whenever you use a web browser to access the internet, data about your device ("standard device data") is sent to the websites you visit and online services you use. Standard device data includes your device's IP address,

browser type and language, access times, and referring website addresses. This data might be logged on those websites' web servers. Which data is logged and how that data is used depends on the privacy practices of the websites you visit and web services you use. Additionally, Microsoft Edge sends a unique browser ID to certain websites to enable us to develop aggregate data used to improve browser features and services.

Additionally, data about how you use your browser, such as your browsing history, web form data, temporary internet files, and cookies, is stored on your device. You can delete this data from your device using Delete Browsing History.

Microsoft Edge allows you to capture and save content on your device, such as:

- **Web note**. Allows you to create ink and text annotations on the webpages you visit, and clip, save, or share them.
- **Active reading**. Allows you to create and manage reading lists, including websites or documents.

- **Hub**. Allows you to easily manage your reading lists, favorites, downloads, and history all in one area.
- **Website Pin to Taskbar**. Allows you to pin your favorite websites to the Windows taskbar. Websites will be able to see which of their webpages you have pinned, so they can provide you a notification badge letting you know there is something new for you to check out on their websites.

Some Microsoft browser information saved on your device will be synced across other devices when you sign in with your Microsoft account. For instance, in Internet Explorer, this information includes your browsing history and favorites; and in Microsoft Edge, it includes your favorites, reading lists, autofill form entries (such as your name, address, and phone number), and may include data for extensions that you have installed. As an example, if you sync your Microsoft Edge reading list across devices, copies of the content you choose to save to your reading list will be sent to each synced device for later viewing. You can disable syncing in Internet

Explorer by going to **Start** > **Settings** > **Accounts** > **Sync your settings**. (For more information, see the Sync settings section of this privacy statement.) You can also disable syncing of Microsoft Edge browser information by turning off the sync option in Microsoft Edge Settings.

Microsoft Edge and Internet Explorer use your search queries and browsing history to provide you with faster browsing and more relevant search results. These features include:

- **Search suggestions** in Internet Explorer automatically sends the information you type into the browser address bar to your default search provider (such as Bing) to offer search recommendations as you type each character.
- **Search and site suggestions** in Microsoft Edge automatically sends the information you type into the browser address bar to Bing (even if you have selected another default search provider) to offer search recommendations as you type each character.

You can turn off these features at any time. In order to provide search results, Microsoft Edge and Internet Explorer send your search queries, standard device information, and location (if you have location enabled) to your default search provider. If Bing is your default search provider, we use this data as described in the Bing section of this privacy statement.

Cortana can assist you with your web browsing in Microsoft Edge with features such as Ask Cortana. You can disable Cortana assistance in Microsoft Edge at any time in Microsoft Edge Settings. To learn more about how Cortana uses data and how you can control that, go to the Cortana section of this privacy statement.

Windows apps

A number of Microsoft apps are included with Windows and others are available in Microsoft Store. Some of those apps include:

Maps app. The Maps app provides location-based services and uses Bing services to process your searches within the Maps app.

When the Maps app has access to your location, and you have enabled location-based services in Windows, when you use the “@” key to initiate a search in supported text boxes in Windows apps, Bing services collects the text you type after the “@” key to provide location-based suggestions. To learn more about these Bing-powered experiences, see the Bing section of this privacy statement. When the Maps app has access to your location, even when the app is not in use, Microsoft may collect de-identified location data from your device to improve Microsoft services. You can disable the Maps app's access to your location by turning off the location service or turning off the Maps app's access to the location service.

You can keep track of your favorite places and recent map searches in the Maps app. Your favorite places and search history will be included as search suggestions. If you're signed in with your Microsoft account, your favorite places, search history, and certain app settings will be synced across other devices and services (for example, Cortana). For more

information, see the Sync and backup settings section of this privacy statement.

Camera app. If you allow the Camera app to use your location, location data is embedded in the photos and videos you take with your device. Other descriptive data, such as camera model and the date that the picture or video was taken, is also embedded in photos and videos. If you choose to share a photo or video, any embedded data will be accessible to the people and services you share with. Once enabled, you can always disable the Camera app's access to your location by turning off all access to the location service in your device's Settings menu or turning off the Camera app's access to the location service.

When the Camera app is open, it shows rectangles detected by the selected camera for areas in the image that are potentially used for image enhancement. The Camera app does not retain any image enhancing data. You can always change your camera access settings in the Camera app’s Settings menu or the Windows Settings menu.

Photos app. There are two versions of the Photos app available. The updated Photos app includes features like iCloud integration and local and cloud folder views. The previous legacy version of the Photos app includes features like Video Editor, the People tab, and Albums. You are using the updated Photos app if the “About” section in the Photos app settings indicates the app is the “Updated” Photos app. In some cases, a user may have both the updated Photos app and the Photos legacy version downloaded on their device.

The updated Photos app helps you organize, view, and share your photos and videos. For example, the Photos app presents different ways to group photos and videos by name, date taken, or date modified, and also in folders where those files are stored, such as stored locally on your device or synced to your device from OneDrive, iCloud, and other cloud services. The app also allows you to move, copy or upload files to different locations on your computer or to OneDrive. The All Photos tab displays your locally stored or synced photos and videos according to the date they

are taken. The Favorites tab lets you view photos and videos you previously liked or favorited. The Folders tab allows you to view photos or videos by their storage location. There are also tabs where you can see your photos and videos from available cloud services (such as OneDrive and other third-party services) that you have synced to your device.

The Photos legacy app also helps you organize, view, and share your photos and videos. However, if you are using the Photos legacy app, you may see other features that are not available in the newer version of the Photos app, including Collections, Albums, Video Editor and the People setting. The Collection tab displays photos and videos according to the date they are taken. The Albums tab helps you organize your photos and videos by location and common tags. The Video Editor allows you to edit, create, and share videos.

The People setting can be enabled on the Photos legacy app's Settings page and in the

People tab of the app. When enabled, the Photos legacy app will use face grouping technology to organize your photos and videos into groups. The grouping feature can detect faces in a photo or video and determine whether they are visually similar to faces in other photos and videos in your local photo collection. You can choose to associate a facial grouping with a contact from your People app.

When enabled in the Photos legacy app, your groupings will be stored on your device for as long as you choose to keep the groupings or the photos or videos. If the People setting is turned on, there will be a prompt to allow the Photos legacy app to continue to permit facial groupings after three years of non-interaction with the Photos legacy app. At any time, you can go to the Settings page in the Photos legacy app to turn the People setting on or off. Turning the feature off will remove facial grouping data from the Photos legacy app but will not remove your photos or videos. Learn more about the Photos legacy app and facial grouping.

If you choose to share a photo or video using the Photos app or the Photos legacy app, any embedded data (such as location, camera model, and date) will be accessible to the people and services you share the photo or video with.

People app. The People app lets you see and interact with all your contacts in one place. When you add an account to the People app, your contacts from your account will be automatically added to the People app. You can add other accounts to the People app, including your social networks (such as Facebook and Twitter) and email accounts. When you add an account, we tell you what data the People app can import or sync with the particular service and let you choose what you want to add. Other apps you install may also sync data to the People app, including providing additional details to existing contacts. When you view a contact in the People app, information about your recent interactions with the contact (such as emails and calendar events, including from apps that the People app syncs data from) will be

retrieved and displayed to you. You can remove an account from the People app at any time.

Mail and Calendar app. The Mail and Calendar app allows you to connect all your email, calendars, and files in one place, including those from third-party email and file storage providers. The app provides location-based services, such as weather information in your calendar, but you can disable the app's use of your location. When you add an account to the Mail and Calendar app, your email, calendar items, files, contacts, and other settings from your account will automatically sync to your device and to Microsoft servers. At any time, you can remove an account or make changes to the data that's synced from your account. To configure an account, you must provide the app with the account credentials (such as user name and password), which will be sent over the internet to the third-party provider's server. The app will first attempt to use a secure (SSL) connection to configure your account but will send this information unencrypted if your email provider does not support SSL. If you

add an account provided by an organization (such as a company email address), the owner of the organizational domain can implement certain policies and controls (for example, multi-factor authentication or the ability to remotely wipe data from your device) that may affect your use of the app.

Messaging app. When you sign in with a Microsoft account on your device, you can choose to back up your information, which will sync your SMS and MMS messages and store them in your Microsoft account. This allows you to retrieve the messages if you lose or change phones. After your initial device set-up, you can manage your messaging settings at any time. Turning off your SMS/MMS backup will not delete messages that have been previously backed up to your Microsoft account. To delete such messages, you must first delete them from your device prior to turning off backup. If you allow the Messaging app to use your location, you can attach a link to your current location to an outgoing message. Location information will be collected by Microsoft as described in the

Windows Location services section of this privacy statement.

Narrator. Narrator is a screen-reading app that helps you use Windows without a screen. Narrator offers intelligent image and page title description and web page summaries when you encounter undescribed images and ambiguous links.

When you choose to get an image description by pressing Narrator + Ctrl + D, the image will be sent to Microsoft to perform analysis of the image and generate a description. Images are used only to generate the description and are not stored by Microsoft.

When you choose to get page title descriptions by pressing Narrator + Ctrl + D, the URL of the site you are visiting will be sent to Microsoft to generate the page title description and to provide and improve Microsoft services, such as Bing services as described in the Bing section above.

When you choose to get a list of popular links for a web page by pressing Narrator + double press of S, the URL of the site you are visiting

will be sent to Microsoft to generate the summary of popular links and to provide and improve Microsoft services, such as Bing.

You can disable these features at any time by going to **Narrator > Get image descriptions, page titles and popular links** in the Windows setting app.

You can also send feedback about Narrator to help Microsoft diagnose and resolve problems with Narrator and improve Microsoft products and services, such as Windows. Verbal feedback can be submitted at any time in Narrator by using Narrator Key + Alt + F. When you use this command, the Feedback Hub app will launch, giving you the opportunity to submit verbal feedback. If you enable the setting “Help Make Narrator Better” in the Windows settings app and submit verbal feedback through Feedback Hub, recent device and usage data, including event trace log (ETL) data, will be submitted along with your verbal feedback to improve Microsoft products and services, such as Windows.

Live captions. Live captions transcribe audio to help with the comprehension of spoken content. Live captions can generate captions from any audio containing speech, whether the audio is online, audio you have downloaded to your device, or audio received from your microphone. By default, transcribing microphone audio is disabled.

Voice data that is captioned is only processed on your device and is not shared to the cloud or with Microsoft. Learn more about live captions.

Windows Media Player

Windows Media Player allows you to play CDs, DVDs, and other digital content (such as WMA and MP3 files), rip CDs, and manage your media library. To enrich your experience when you play content in your library, Windows Media player displays related media information, such as album title, song titles, album art, artist, and composer. To augment your media information, Windows Media player will send a request to Microsoft which contains standard computer information, an

identifier for the media content, and the media information already contained in your Windows Media Player library (including information you may have edited or entered yourself) so that Microsoft can recognize the track and then return additional information that is available.

Windows Media Player also allows you to play back content that is streamed to you over a network. To provide this service, it is necessary for Windows Media Player to communicate with a streaming media server. These servers are typically operated by non-Microsoft content providers. During playback of streaming media, Windows Media Player will send a log to the streaming media server or other web server(s) if the streaming media server requests it. The log includes such details as: connection time, IP address, operating system version, Windows Media Player version, Player identification number (Player ID), date, and protocol. To protect your privacy, Windows Media Player defaults to sending a Player ID that is different for each session.

Windows Hello

Windows Hello provides instant access to your devices through biometric authentication. If you turn it on, Windows Hello uses your face, fingerprint, or iris to identify you based on a set of unique points or features that are extracted from the image and stored on your device as a template—but it does not store the actual image of your face, fingerprint, or iris. Biometric verification data that's used when you sign in doesn't leave your device. Your biometric verification data will remain on your device until you remove it. However, after a significant period of Windows Hello inactivity, you will be prompted to confirm that you want to continue to store your biometric verification data. You can delete your biometric verification data from within Settings. Learn more about Windows Hello.

Windows Search

Windows Search lets you search your stuff and the web from one place. If you choose to use Windows Search to search "your stuff," it will

provide results for items on your personal OneDrive, your OneDrive for Business if so enabled, other cloud storage providers to the extent supported by those third-party providers, and on your device. If you choose to use Windows Search to search the web, or get search suggestions with Windows Search, your search results will be powered by Bing and we will use your search query as described in the Bing section of this privacy statement. Learn more about search in Windows.

Entertainment and related services

Entertainment and Related Services power rich experiences and enable you to access a variety of content, applications and games.

Xbox

The Xbox network is the online gaming and entertainment service from Microsoft that consists of software and enables online experiences across different platforms. This service lets you find and play games, view content, and connect with friends on Xbox and

other gaming and social networks. You can connect to the Xbox network using Xbox consoles, Windows devices, and mobile devices (Android and iPhone).

When you sign up for an Xbox profile, we assign you a gamertag (a public nickname) and a unique identifier. When you sign in on Xbox devices, apps, and services, the data we collect about your use is stored using these unique identifier(s).

Xbox consoles are devices you can use to find and play games, movies, music, and other digital entertainment. When you sign in to Xbox experiences—in apps or on a console—we also assign a unique identifier to your device. When your Xbox console is connected to the internet, for instance, and you sign in to the console, we identify which console and which version of the console's operating system you're using.

Xbox continues to provide new experiences in client apps that are connected to and backed by services such as the Xbox network and cloud gaming. When signed in to an Xbox

experience, we collect required data to help keep these experiences reliable, up to date, secure, and performing as expected.

Data we collect about your use of Xbox services, games, apps, and consoles includes:

- When you sign in and sign out of Xbox, any purchases you make, and content you obtain.
- Which games you play and apps you use, your game progress, achievements, play time per game, and other play statistics.
- Performance data about Xbox consoles, Xbox Game Pass and other Xbox apps, the Xbox network, connected accessories, and your network connection, including any software or hardware errors.
- Content you add, upload, or share through the Xbox network, including text, pictures, and video you capture in games and apps.
- Social activity, including chat data and interactions with other gamers, and connections you make (friends you add and people who follow you) on the Xbox network.

If you use an Xbox console or Xbox app on another device capable of accessing the Xbox network, and that device includes a storage device (hard drive or memory unit), usage data will be stored on the storage device and sent to Microsoft the next time you sign in to Xbox, even if you've been playing offline.

Xbox console diagnostic data. Diagnostic data has two categories: required and optional. If you use an Xbox console, the console will send required data to Microsoft. Optional data is additional data that you choose to share with Microsoft.

- **Required**. The minimum data necessary to help keep Xbox safe, secure, up to date, and performing as expected.
- **Optional**. Optional data includes additional details about your console, its settings, its health, its use, and enhanced error reporting to help us detect, diagnose, and fix problems.

Learn more at Manage settings for optional data sharing.

Game captures. Any player in a multiplayer game session can record video (game clips) and capture screenshots of their view of the game play. Other players' game clips and screenshots can capture your in-game character and gamertag during that session. If a player captures game clips and screenshots on a PC, the resulting game clips might also capture audio chat.

Captioning. During Xbox real-time ("party") chat, players may activate a voice-to-text feature that lets them view that chat as text. If a player activates this feature, all voice communication in the party is captioned for the player. Microsoft uses the resulting text data to provide captioning of chat for players who need it, as well as the other purposes described in this statement.

Data use. Microsoft uses the data we collect to improve gaming products and experiences—making them safer and more fun over time.

Data we collect also enables us to provide you with personalized, curated experiences. This includes connecting you to games, content,

and services, as well as presenting you with offers, discounts, and recommendations.

Xbox data viewable by others. Your gamertag, game and play statistics, achievements, presence (whether you are currently signed in to Xbox), content you share, and other data about your activity on Xbox can be seen by:

- Other players signed in to Xbox.
- Customers of third-party services you've linked your profile to, or
- Other services associated with Xbox (including those of partner companies).

For example, your gamertag and scores that show on game leaderboards are considered public and cannot be hidden. For other data, you can adjust your privacy settings on consoles and at Xbox.com to limit or block what is shared with the public or with friends.

Learn more at Xbox online safety and privacy settings.

Xbox data shared with third parties including game and apps publishers. When you use an Xbox online game or any network-connected

app on your Xbox console, PC, or mobile device, the publisher of that game or app has access to data about your usage to help the publisher deliver, support, and improve its product. This data may include: your Xbox user identifier, gamertag, limited account info such as country and age range, data about your in-game communications, any Xbox enforcement activity, game-play sessions (for example, moves made in-game, types of vehicles used in-game), your presence on the Xbox network, the time you spend playing the game or app, rankings, statistics, gamer profiles, avatars, or gamerpics, friends lists, activity feeds for official clubs you belong to, official club memberships, and any content you create or submit in the game or app.

Third-party publishers and developers of games and apps have their own distinct and independent relationship with users and their collection and usage of personal data is subject to their specific privacy policies. You should carefully review their policies to determine how they use the data. For example, publishers may choose to disclose or display

game data (such as on leaderboards) through their own services. You may find their policies linked from game or app detail pages in the Microsoft Store.

Learn more at Data Sharing with Games and Apps.

To stop sharing game or app data with a publisher, remove its games or app from all devices where you have installed them. Some publisher access to your data may be revoked at https://microsoft.com/consent.

Children and family. If you have kids who want to use the Xbox network, you can set up child and teen profiles for them once they have Microsoft accounts. Adult organizers in your Microsoft family group can change consent choices and online safety settings for child and teen profiles on Xbox.com.

Learn more about Microsoft family groups at Simplify your family's life.

Learn more about managing Xbox profiles, at Xbox online safety and privacy settings.

For more information about Microsoft's collection of data from children, including Xbox, please see the Collection of data from children section of this privacy statement.

Safety. In order to help make the Xbox network a safe gaming environment and enforce the Community Standards for Xbox, we may collect and review voice, text, images, videos and in-game content (such as game clips you upload, conversations you have, and things you post in clubs and games).

Anti-cheat and fraud prevention. Providing a fair gameplay environment is important to us. We prohibit cheating, hacking, account stealing, and any other unauthorized or fraudulent activity when you use an Xbox online game or any network-connected app on your Xbox console, PC, or mobile device. In order to detect and prevent fraud and cheating, we may use anti-cheat and fraud prevention tools, applications, and other technologies. Such technologies may create digital signatures (known as "hashes") using certain information collected from your Xbox console,

PC, or mobile device, and how you use that device. This can include information about the browser, device, activities, game identifiers, and operating system.

Legacy.

- **Xbox 360**. This Xbox console collects limited required diagnostic data to keep your console functioning as expected while using a console connected to the Xbox network.
- **Kinect**. The Kinect sensor is a combination of camera, microphone, and infrared sensor that can enable motions and voice to be used to control gameplay. For example:
  - If you choose, the camera can be used to sign you in to the Xbox network automatically using facial recognition. This data stays on the console and is not shared with anyone, and you can choose to delete this data from your console at any time.
  - For game play, Kinect will map distances between your body's joints to create a

stick figure representation of you that helps Kinect enable play.
    - The Kinect microphone can enable voice chat between players during play. The microphone also enables voice commands for control of the console, game, or app, or to enter search terms.
    - The Kinect sensor can also be used for audio and video communications through services such as Skype.

Learn more about Kinect at Xbox Kinect and Privacy.

Microsoft Store

Microsoft Store is an online service, accessible via PC, the Xbox Console and the Xbox App, that allows you to browse, download, purchase, rate, and review applications and other digital content. It includes:

- Apps and content for Windows devices such as phones, PCs, and tablets.
- Games, subscriptions and other apps for Xbox consoles and other devices.

- Products and apps for Microsoft 365, SharePoint, Exchange, Access, and Project (2013 versions or later).

We collect data about how you access and use Microsoft Store; the products you've viewed, purchased, or installed; the preferences you set for viewing apps in Microsoft Store; and any ratings, reviews, or problem reports you submit. Your Microsoft account is associated with your ratings and reviews; and if you write a review, the name and picture from your Microsoft account will be published with your review.

Permission for Microsoft Store apps. Many apps you install from the Microsoft Store are designed to take advantage of specific hardware and software features of your device. An app's use of certain hardware and software features may give the app or its related service access to your data. For example, a photo editing app might access your device's camera to let you take a new photo or access photos or videos stored on your device for editing, and a restaurant guide

might use your location to provide nearby recommendations. Information about the features that an app uses is provided on the app's product description page in Microsoft Store. Many of the features that Microsoft Store apps use can be turned on or off through your device's privacy settings. In Windows, in many cases, you can choose which apps can use a particular feature. Go to **Start > Settings > Privacy or Privacy & Security**, select the feature (for example, Calendar), and then select which app permissions are on or off. The lists of apps in Windows privacy settings that can use hardware and software features will not include "Classic Windows" applications, and these applications are not affected by these settings.

App updates. Unless you have turned off automatic app updates in the relevant Microsoft Store settings or have acquired an app provided and updated by the app developer, Microsoft Store will automatically check for, download, and install app updates to verify that you have the latest versions. Updated apps might use different Windows

hardware and software features from the previous versions, which could give them access to different data on your device. You will be prompted for consent if an updated app accesses certain features, such as location. You can also review the hardware and software features an app uses by viewing its product description page in Microsoft Store.

Each app's use of your data collected through any of these features is subject to the app developer's privacy policies. If an app available through Microsoft Store collects and uses any of your personal data, the app developer is required to provide a privacy policy, and a link to the privacy policy is available on the app's product description page in Microsoft Store.

Sideloaded apps and developer mode. Developer features such as the "developer mode" setting are intended for development use only. If you enable developer features, your device may become unreliable or unusable, and expose you to security risks. Downloading or otherwise acquiring apps from sources other than Microsoft Store, also known as

"sideloading" apps, may make your device and personal data more vulnerable to attack or unexpected use by apps. Windows policies, notifications, permissions, and other features intended to help protect your privacy when apps access your data may not function as described in this statement for sideloaded apps or when developer features are enabled.

Microsoft Start

Microsoft Start is a content service that includes news, weather, sports, and finance. The Microsoft Start app is available on various platforms, including iOS and Android. The Microsoft Start service is also included within other Microsoft services, including the Microsoft Edge browser and widgets on Windows.

When you install the Microsoft Start app, we collect data that tells us if the app was installed properly, the installation date, the app version, and other data about your device such as the operating system and browser. This data is collected on a regular basis to help us determine the number of Microsoft Start app

users and identify performance issues associated with different app versions, operating systems, and browsers.

We also collect data about how you interact with Microsoft Start content, such as usage frequency and articles viewed, to provide you with relevant content. Microsoft Start provides an enhanced experience when you sign in with your Microsoft account, including allowing you to customize your interests and favorites. You can manage personalization through Microsoft Start and Bing settings, as well as through settings in other Microsoft services that include Microsoft Start services. We also use the data we collect to provide you with advertisements that may be of interest to you. You can opt out of interest-based advertising through the advertising links within Microsoft Start services, or by visiting the Microsoft opt-out page.

Previous versions of MSN Money allow you to access personal finance information from third-party financial institutions. MSN Money only displays this information and does not

store it on our servers. Your sign-in credentials used to access your financial information from third parties are encrypted on your device and are not sent to Microsoft. These financial institutions, as well as any other third-party services you access through MSN services, are subject to their own terms and privacy policies.

Groove Music and Movies & TV

Groove Music lets you easily play your music collection and make playlists. Microsoft Movies & TV allows you to play your video collection and rent or buy movies and TV episodes. These services were formerly offered as Xbox Music and Video.

To help you discover content that may interest you, Microsoft will collect data about what content you play, the length of play, and the rating you give it.

To enrich your experience when playing content, Groove Music and Movies & TV will display related information about the content you play and the content in your music and

video libraries, such as the album title, cover art, song or video title, and other information, where available. To provide this information, Groove Music and Movies & TV send an information request to Microsoft containing standard device data, such as your device IP address, device software version, your regional and language settings, and an identifier for the content.

If you use Movies & TV to access content that has been protected with Microsoft Digital Rights Management (DRM), it may automatically request media usage rights from an online rights server and download and install DRM updates in order to let you play the content. See the DRM information in the Silverlight section of this privacy statement for more information.

Silverlight

Microsoft Silverlight helps you to access and enjoy rich content on the Web. Silverlight enables websites and services to store data on your device. Other Silverlight features involve connecting to Microsoft to obtain updates, or

to Microsoft or third-party servers to play protected digital content.

Silverlight Configuration tool. You can make choices about these features in the Silverlight Configuration tool. To access the Silverlight Configuration tool, right click on content that is currently being displayed by Silverlight and select **Silverlight**. You can also run the Silverlight Configuration tool directly. In Windows, for example, you can access the tool by searching for "Microsoft Silverlight."

Silverlight application storage. Silverlight-based applications can store data files locally on your computer for a variety of purposes, including saving your custom settings, storing large files for graphically intensive features (such as games, maps, and images), and storing content that you create within certain applications. You can turn off or configure application storage in the Silverlight Configuration tool.

Silverlight updates. Silverlight will periodically check a Microsoft server for updates to provide you with the latest features and

improvements. A small file containing information about the latest Silverlight version will be downloaded to your computer and compared to your currently installed version. If a newer version is available, it will be downloaded and installed on your computer. You can turn off or configure updates in the Silverlight Configuration tool.

Digital Rights Management. Silverlight uses Microsoft Digital Rights Management (DRM) technology to help protect the rights of content owners. If you access DRM-protected content (such as music or video) with Silverlight, it will request media usage rights from a rights server on the Internet. In order to provide a seamless playback experience, you will not be prompted before Silverlight sends the request to the rights server. When requesting media usage rights, Silverlight will provide the rights server with an ID for the DRM-protected content file and basic data about your device, including data about the DRM components on your device such as their revision and security levels, and a unique identifier for your device.

DRM updates. In some cases, accessing DRM-protected content will require an update to Silverlight or to the DRM components on your device. When you attempt to play content that requires a DRM update, Silverlight will send a request to a Microsoft server containing basic data about your device, including information about the DRM components on your computer such as their revision and security levels, troubleshooting data, and a unique identifier for your device. The Microsoft server uses this identifier to return a unique DRM update for your device, which will then be installed by Silverlight. You can turn off or configure DRM component updates on the **Playback** tab in the Silverlight Configuration tool.

Windows Mixed Reality

Windows Mixed Reality allows you to enable a virtual reality experience that immerses you in apps and games. Mixed Reality uses a compatible headset's camera, microphone, and infrared sensors to enable motions and voice to be used to control gameplay and to navigate apps and games.

Microsoft collects diagnostic data to solve problems and to keep Mixed Reality running on Windows up to date, secure, and operating properly. Diagnostic data also helps us improve Mixed Reality and related Microsoft products and services depending on the diagnostic data settings you've chosen for your device. Learn more about Windows diagnostic data.

Mixed Reality also processes and collects data specifically related to the Mixed Reality experiences, such as:

- Mixed Reality maps distances between your body's joints to create a stick figure representation of you. If you are connected to the Internet, we collect those numeric values to enable and improve your experience.
- Mixed Reality detects specific hand gestures intended to perform simple system interactions (such as menu navigation, pan/zoom, and scroll). This data is processed on your PC and is not stored.

- The headset's microphones enable voice commands to control games, apps, or to enter search terms. Learn more about voice data collection.
- Windows Mixed Reality can also be used for audio and video communications through services such as Skype.

Your Privacy Choices

- Sitemap
- Contact Microsoft
- Privacy
- Manage cookies
- Terms of use
- Trademarks
- Safety & eco
- Recycling
- About our ads
-