



# Microsoft Privacy Statement

Last Updated: February 2020 [What's new?](#)

Your privacy is important to us. This privacy statement explains the personal data Microsoft processes, how Microsoft processes it, and for what purposes.

Microsoft offers a wide range of products, including server products used to help operate enterprises worldwide, devices you use in your home, software that students use at school, and services developers use to create and host what's next. References to Microsoft products in this statement include Microsoft services, websites, apps, software, servers, and devices.

Please read the product-specific details in this privacy statement, which provide additional relevant information. This statement applies to the interactions Microsoft has with you and the Microsoft products listed below, as well as other Microsoft products that display this statement.

## 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, purchase an MSDN subscription, sign up for Office 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, such as skills related to Cortana.
- Publicly-available sources, such as open government databases.

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 third party bots and skills available through Microsoft products like Cortana.
- **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.
- **Voice data.** Your voice data, such as the search queries or commands 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 Xbox Live, 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.

**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.

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, our automated methods include artificial intelligence (AI), which we think of as a set of technologies that enable computers to perceive, learn, reason, and assist in decision-making to solve problems in ways that are similar to what people do. To build, train, and improve the accuracy of our automated methods of processing (including 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 example, we manually review short snippets of a small sampling of voice data we have taken steps to de-identify to improve our speech services, such as recognition and translation.

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 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 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.
- **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 ensure 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, 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 products, and on third-party web properties, for advertising in our products 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.
- **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 ensure we meet 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.

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 interest-based 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.

- **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.
- **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](#).
- **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](#).
- **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](#).
- **Xbox.** If you use Xbox Live 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.
- **Microsoft Store.** You can access your Microsoft Store profile and account information by visiting [Microsoft Store](#) and selecting **View account** or **Order history**.
- **Microsoft.com.** You can access and update your profile on microsoft.com by visiting your [Microsoft account profile page](#).
- If you have a **Microsoft Developer Network (MSDN)** public profile, you can access and edit your data by signing in at [MSDN forum](#).

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 within 30 days.

## 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 interest-based 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, if you enter your city or postal code to get local news or weather information on a Microsoft website, depending on your settings, 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.
- **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 don't 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 ensure that our websites remain up and running.

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:

- **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, MSPPProf.** 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.** Used to collect information for analytics purposes.
- **x-ms-gateway-slice.** Identifies a gateway for load balancing.
- **TOptOut.** Records your decision not to receive interest-based advertising delivered by Microsoft.

In addition to the cookies Microsoft sets when you visit our websites, 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. See opt-out links below.
- Companies that deliver content, such as videos or news, or ads on Microsoft sites, 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.

## 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. .

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 clicking any of the following links: [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 provided by an organization you are affiliated with, such as an employer or school, and you use your work or school account to access that Microsoft product, 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 for Microsoft's legitimate 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 legitimate business operations in connection with providing products to your organization, please contact Microsoft as described in the [How to contact us](#) section. For more information on our legitimate 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 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 Xbox Live).

- **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. 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.
- **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 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.**

## 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, Chile, 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 ensure that the data we collect under this privacy statement is processed according to the provisions of this statement and the requirements of applicable law wherever the data is located.

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, to help ensure your rights and protections 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. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, the United Kingdom, and Switzerland to the United States. Microsoft Corporation has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If third-party agents process personal data on our behalf in a manner inconsistent with the principles of either Privacy Shield framework, we remain liable unless we prove we are not responsible for the event giving rise to the damage. The controlled U.S. subsidiaries of Microsoft Corporation, as identified in our self-certification submission, also adhere to the Privacy Shield Principles—for more info, see the list of [Microsoft U.S. entities or subsidiaries adhering to the Privacy Shield Principles](#).

If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, visit the [Privacy Shield website](#).

If you have a question or complaint related to participation by Microsoft in the EU-U.S. or Swiss-U.S. Privacy Shield, we encourage you to contact us via our [web form](#). For any complaints related to the Privacy Shield 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, and with 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 Privacy Shield 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).

## 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.

## California Consumer Privacy Act

---

If you are a California resident, we process your personal data in accordance with the California Consumer Privacy Act (CCPA). This CCPA section of our Privacy Statement contains information required by the CCPA and supplements our Privacy Statement.

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

**Rights.** You have the right to request that we (i) disclose what personal data we collect, use, disclose, and sell and (ii) delete your personal data. 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 CCPA rights.

If you have a Microsoft account, you must 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 or use our [web form](#). 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 have a right not to receive discriminatory treatment if you exercise your CCPA rights. We will not discriminate against you if you exercise your CCPA 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 share the personal data. 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
  - Sources of personal data: Interactions with users and partners with whom we offer co-branded services
  - Purposes of Processing (Collection and Sharing with 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 Sharing with 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 Sharing with 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 Sharing with 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 Sharing with 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 Sharing with 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 Sharing with 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 Sharing with 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 Sharing with 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.

**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.

## Advertising

---

Advertising allows us to provide, support, and improve some of our products. Microsoft does not use what you say in email, 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 in our products 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](#), MSN, and Bing.
- When the advertising ID is enabled in Windows 10 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 partners, such as Verizon Media, AppNexus, 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 MSN 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 MSN. 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](https://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 16 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.
- **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 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: [AppNexus](#), [Facebook](#), [Media.net](#), [Outbrain](#), [Taboola](#) and [Verizon Media](#). 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.

#### Collection of data from children

---

When a Microsoft product collects age, and there is an age in your jurisdiction under which parental consent or authorization is required to use the product, the product will either block users under that age or will ask them to provide consent or authorization from a parent or guardian before they can use it. 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.



Parents can change or revoke the consent choices previously made, and review, edit, or request the deletion of the personal data of children for whom they provided consent or authorization. For example, parents can access their personal [Microsoft account](#) and select **Permissions**. For users of Minecraft for PC/Java and other Mojang games, parents can visit the [Mojang Account page](#).

## 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 EU Data Protection Officer, please contact us by using our [web form](#). We will respond to questions or concerns within 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](#).

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](#).

## 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 [Microsoft Online Services Terms](#) (OST), such as 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 cloud-based services, such as PlayFab Services and tools such as Cortana Skills Kit.
- 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 OST 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 [OST](#), 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 legitimate 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 [Online Services Terms \(OST\)](#) 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, (b) Microsoft is processing Personal Data for its legitimate business operations, in which case Microsoft is a controller, or (c) stated otherwise in the [OST](#). Microsoft is a controller of Personal Data when processing Personal Data for its legitimate business operations associated with providing the service, such as billing and preparing invoices; account management; compensation; financial reporting; business planning and product strategy; improving core functionality for accessibility, privacy, and energy efficiency; and combatting fraud, cybercrime, and cyberattacks on Microsoft products. We generally aggregate Personal Data before using it for our legitimate business operations, removing the ability to identify specific individuals. We use personal data in the least identifiable form that will support processing necessary for legitimate business operations.

**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 OST.

Some Enterprise Online Services require, or are enhanced by, the installation of local software (e.g., agents, device management applications) on a device. At your direction, the local software may transmit (i) data, which can include Customer Data, from a device or appliance to or from the Enterprise Online Services; or (ii) logs or error reports to Microsoft for troubleshooting purposes. The Enterprise Online Services, including local software, collect device and usage data that is transmitted to Microsoft and analyzed to improve the quality, security, and integrity of our products.

Bing Search Services, as defined in the OST, 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.

#### 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.

##### Office

---

Office is a collection of productivity services and applications including Word, Excel, PowerPoint, and Outlook, among others. For more details about Outlook, see the [Outlook](#) section of this privacy statement. Office is a service that is comprised of client software applications and connected online services that span many platforms and have numerous interdependent experiences. Various Office 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. Prior to Office 365 version 1904, you can change your privacy settings in the Privacy Options of the Microsoft Office Trust Center. For more information, see [View my options and settings in the Microsoft Office Trust Center](#). Starting with Version 1904 of Office 365, you can access new, updated, and improved privacy controls by selecting **File > Account > Account Privacy**. See [Account Privacy Settings](#) for more information.

**Office Roaming Service.** The Office Roaming Service helps keep your Office settings up to date across your devices running Office. When you sign in to Office with your Microsoft account or an account issued by your organization, the Office Client Policy Service is turned on and syncs some of your customized Office settings to Microsoft servers (such as a list of most recently used documents and the last location viewed within a document). When you sign in to Office on another device with the same account, the Office Roaming Service downloads your settings from Microsoft servers and applies them to the additional device. The Office Roaming Service also applies some of your customized Office settings when you sign in to Office.com. When you sign out of Office, the Office Roaming Service removes your Office settings from your device. Any changes you made to your customized Office settings are sent to Microsoft servers.

**Microsoft Updates.** Office uses either Microsoft Update or Click-to-Run services to provide you with security and other important updates. See the [Update Services](#) section of this privacy statement for more information about Microsoft Update.

**Click-to-Run Update Service.** The Click-to-Run Update Service allows you to install certain Microsoft Office products over the internet. The Click-to-Run Update Service also automatically detects online updates to Click-to-Run-enabled products on your device and downloads and installs them automatically.

**Office Translator.** Office Translator is designed as a no-trace connected experience. With [no trace](#), no portion of your translation request that Office sends to Microsoft Translator will be logged, your submitted text will not be used to improve the quality of the Microsoft Translator service, and there will not be any record of any portion of your data retained by Microsoft.

**Diagnostic Data.** Diagnostic data is used to (i) keep Office 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 Office. Users have a choice between two different levels of diagnostic data collection, Required and Optional.

- **Required.** The minimum data necessary to help keep Office 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 in Office](#) for more information.

**Connected Experiences.** Office continues to provide more experiences in client applications that are connected to and backed by cloud-based services. In order to ensure that all these connected experiences will be reliable, up to date, remain secure, and perform as expected, required service data may be collected whenever you use a connected experience.



Office consists of client software applications and connected experiences designed to enable you to create, communicate, and collaborate more effectively. Working with others on a document stored on OneDrive for Business 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 Office 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, Office templates or PowerPoint QuickStarter.

Prior to Office 365 version 1904, you can change your privacy settings in the Privacy Options of the Microsoft Office Trust Center.

Starting with Version 1904 of Office 365, you can access new, updated, and improved privacy controls by selecting **File > Account > Account Privacy**. 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 Office functionality will remain available, such as syncing your mailbox in Outlook, as well as essential services described below.

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.

There are a set of services that are essential to how Office functions and cannot be disabled. For example, the licensing service that confirms that you are properly licensed to use Office 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**

Required service data is data that enables us to deliver cloud-based connected experiences and help make these experiences secure and perform as expected. There are three types of information that are considered as required service data.

- **Customer Content**, which is content you create using Office, such as text typed in a Word document.
- **Functional Data**, which includes information needed by a connected experience to perform its task, such as configuration information about the app.
- **Service Diagnostic Data**, which is the data required to keep the service secure, up to date, and performing as expected. Because this data is strictly related to the connected experience, it is separate from Required or Optional diagnostic data levels.

To help you understand required service data, the following is an example scenario using PowerPoint Designer, which is a connected experience you can use when creating slides for a presentation. PowerPoint Designer helps you improve your slides by automatically generating design ideas to choose from. While you're putting content on a slide, Designer works in the background to match that content to professionally designed layouts.



The required service data that is sent to Microsoft to enable this connected experience for you could include the following:

- Customer content, such as the text or images you added to your slide.
- Functional data, such as which slide you are working on and its layout.
- Service diagnostic data, such as events that tell us if the design idea was correctly applied to your slide and that the service calls were performing correctly.

If you choose to disable the category of connected experiences that includes PowerPoint Designer, the feature will be turned off and none of this required service data is sent to us.

See [Connected Experiences in Office](#) for more information

## 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 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 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 [Office](#) 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 directory and may be recommended to other

users. Your profile includes your user name, avatar, and any other data you choose to add to your profile or display to others.

**Skype Contacts.** If you use a Microsoft service, such as Outlook.com, to manage contacts, Skype will automatically add the people you know to your Skype contact list until you tell us to stop. With your permission, Skype will also check your device or other address books to automatically add your friends as Skype contacts. You can block users if you don't want to receive their communications.

**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 don't 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.** To help you communicate with people in different languages, some Skype apps offer audio and/or text translation features. When you use translation features, your voice and text data are used to provide and improve Microsoft speech recognition and translation services.

**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 includes whether you need to get consent from all parties to the communication in advance.** 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.

**Recommendations in Skype.** Subject to availability, Skype may offer suggestions to help you manage your time, tasks, find information and get things done. For example, Skype may provide contextual prompts to create reminders or suggest you create a task using Microsoft services. This data may also be used to improve Microsoft products.

**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.

## 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 the Bing Toolbar and Bing Desktop apps. Bing services collect and process data in many forms, including text that has been inked or typed, speech data, and images. Bing services are also included within other Microsoft services, such as MSN Apps, Office, 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. 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 Ask Cortana or 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.

**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 Windows 10 search box. On Windows, you can always hide the search box so as not to use the feature.

**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 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. Clearing your history prevents that history from being displayed on the Search History site, 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.

**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.

**Search query passed in referral URL.** 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 URL of the site you came from (in this case, the Bing search results page). Because the URL of the Bing search results page contains the text of the search query you entered (which could include names, addresses, or other identifying information), the destination website will be able to determine the search term you entered.

If your browser is enabled to allow pages to pre-load in the background for faster performance, when your browser loads a page in the background, it will have the same effect as if you visited that page, including sending the Bing search results page URL (containing your search query) and downloading any cookies or similar technologies that page sets.



**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 intelligent assistant that provides smart features and personalized experiences across a variety of devices, apps, and services. As described below, the data we collect when you use Cortana depends on the choices you make (including your privacy settings and whether or not you are signed-in), the data you share with Cortana, and Cortana's capabilities (which vary depending on your operating system, device, and the services and apps you use). Cortana works best when you sign in and allow use of data from your device, your Microsoft account, other Microsoft services, and third-party services to which you choose to connect.

You can manage what data Cortana uses or remembers about you in Cortana Settings, Permissions, Notebook, and the [Microsoft privacy dashboard](#). More about Cortana features and how to manage them can be found at [Cortana and privacy](#).

The data Cortana collects is used to provide, improve, personalize, and develop Cortana and other Microsoft products. For example:

- Cortana uses information about your interests to recommend features you may enjoy.
- Cortana shares information with third parties at your direction to complete a task or transaction you've requested, or help you with a skill such as booking a ride share service.
- Microsoft uses your voice data to improve speech recognition and user intent understanding to improve Cortana and other Microsoft products.
- Cortana provides features that may process your personal and work data from other Microsoft products (e.g., Office) or third-party services. For example, when scheduling a meeting, Cortana can help you identify conflicts on both your personal and work calendars.

On Windows devices, if you choose not to sign in to Cortana, you can still chat with Cortana and use Cortana to search, using either your voice, inking, or typing.

When you use Cortana when you are signed out, we collect:

- **Voice data.** To help Cortana better understand the way you speak and your voice commands, we collect voice data and use it to build speech models and improve speech recognition and user intent understanding. If you choose to sign in, the speech models are more personalized.
- **Searches and commands.** We collect your searches and commands to provide, improve, and develop Cortana and other products. Your Bing search queries and the Search Suggestion feature, even if Cortana does the searching for you, are treated like any other Bing search queries and are used as described in the [Bing](#) section of this privacy statement.
- **Device and usage data.** We collect information about your device as well as the hardware and software you use. For example, Cortana can access data about your device and how you use it. For instance, Cortana can determine if Bluetooth is on,



whether you've locked your screen, your alarm settings, and which apps you install and use.

If you sign in with your Microsoft account, you can enable Cortana to perform additional tasks and to provide personalized experiences and suggestions. Cortana can process the demographic data (such as your age, address, and gender) associated with your Microsoft account and data collected through other Microsoft services to provide personalized suggestions. For example, Cortana may send you a time to leave notification based on your schedule and address. Cortana also learns your favorite places from the Microsoft Maps app, and what you view and purchase in Microsoft Store to improve suggestions. Your interests in the Cortana Notebook can be used by other Microsoft services, such as Bing or MSN, to customize your interests, preferences, and favorites in those experiences as well.

When you sign in to Cortana, in addition to the information described above, we also collect:

**Location data.** You can choose whether Cortana processes your location information to give you relevant notices and results and to make suggestions such as local traffic information and location-based reminders. If you grant permission, Cortana will regularly collect and use your current location, location history, and other location signals (such as locations tagged on photos you upload to OneDrive). Location data Cortana collects is used to provide you with personalized experiences across our products, such as making Bing search results more relevant. It may also be used in de-identified form to improve Microsoft's location services.

**Contacts, communications, and other inputs.** You can choose to let Cortana collect and access your device and cloud-based email and other communications, your calendar and tasks, and your contacts to enable additional features and personalization. If you give permission, Cortana will collect and process additional data, including:

- **Contacts, text messages, and email.** Cortana uses your contacts and messages to do a variety of things, such as: making calls in the Teams app, allowing you to add events to your calendar, apprising you of messages or important contacts, and keeping you up to date on events and important activities. Cortana also uses your contacts and messages to help you with planning and offers other suggestions.
- **Communications history.** Cortana learns who is most important to you and your preferred methods of communication by analyzing your call, text message, and email history. Cortana uses this data to flag important messages for you (such as missed calls), and to improve the performance of features such as speech recognition.
- **Calendar appointments.** Cortana uses your calendars to provide reminders and information relevant to your appointments.

**Browse history.** If you choose, Cortana can use the Microsoft Edge browse history associated with your Microsoft account. Cortana uses this data to learn about you and provide you with intelligent answers and timely, personalized suggestions, or to complete web tasks for you. Cortana can also help you pick up where you left off on one device when browsing in Microsoft Edge on another device. Cortana won't collect information about sites you visit in InPrivate tabs.

**Connected services and skills.** To enable greater personalization and productivity, you can give Cortana permission to (i) collect data from other Microsoft and third-party services, and (ii) provide your information to those services. When enabled, Cortana provides your requests and responses to those services or third parties to enable them to provide you their information or services. With your permission, Cortana can send additional information (e.g., your location). Information you share with a third party is governed by the third party's privacy policy and terms. Cortana also uses data about your use of connected

services and skills to improve and develop Cortana and other Microsoft products. For example, we use this data, including your query sent to the third party, to improve speech recognition and user-intent understanding within Microsoft products. Below are examples of how your data is processed when you use connected services and skills:

- If you choose to connect Cortana to your work or school account, Cortana can access data stored in Office 365 to help you stay up to date, manage your email and calendar, and get insights about your meetings and relationships.
- Choosing to connect Cortana to LinkedIn allows Microsoft to access your LinkedIn data so Cortana can give you more personalized information and recommendations. It also enables LinkedIn to access the name, email address, job title, and company name of people you are meeting with to retrieve relevant information about those contacts.
- Cortana allows you to connect to third-party services to do more and get additional experiences from the third-party service. Cortana may also personalize your experiences based on your use of third-party skills. With your permission, **Cortana can send information about you along with your request to third-parties that ask for it.** For instance, when you ask Cortana to request you a ride, the ride provider will ask for your current location. Third-party skills provide their own separate terms and privacy statements. Please review those carefully before allowing Cortana to send information to them.

## 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. 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 and macOS.** Microsoft Edge is the default web browser for Windows 10 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:** which 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. For example, you may choose to sync browser information saved on your device across other devices when you are signed in with your Microsoft account. You may choose which browser data to sync, including your favorites, 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. 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). You can disable or configure syncing in the Microsoft Edge settings.

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.

To improve your web experience, you may choose to share your Microsoft Edge browsing history from your Microsoft account to allow us to personalize advertising, Bing search, Microsoft News and other Microsoft services. For more information about our **advertising privacy policies** see the [Advertising](#) section of the privacy statement. If you disable the **See ads that interest you** setting in the Microsoft privacy dashboard, you will continue to receive personalized search and news based on your browsing history if you enabled the **Improve your web experience by allowing Microsoft to use your browsing history from this account for personalizing advertising, search, news and other Microsoft services** setting in Microsoft Edge. You may disable this browser setting at any time to stop receiving personalized web experiences based on your browsing history.

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.

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, 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](#)

**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 10, 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.

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 designed to automatically translate text and speech between numerous supported languages.

Microsoft Translator (which includes apps for Android, iOS, Windows, Translator Hub, Translator for Bing, and Translator for Microsoft Edge, collectively "Translator") processes the text, image, and speech data you submit, as well as device and usage data. We use this data to provide Translator, personalize your experiences, and improve our products. Microsoft has implemented business and technical measures designed to help de-identify the data you submit to Translator. For example, when we randomly sample text to improve Translator, we delete identifiers and certain text, such as email addresses and some number sequences, detected in the sample that could contain personal data.

For more information on the 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 Office, see the [Productivity and communications products](#) section of this privacy statement.

## SwiftKey

---

SwiftKey Keyboard and related products (collectively, the "SwiftKey Services") process data about how you type and write, 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 prediction.

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 to enable SwiftKey's algorithms to make predictions based on what you type. 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 attempts to avoid collecting sensitive data, such as fields flagged 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 personalization, 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.

SwiftKey Account holders have the option to use the SwiftKey personalization service, which more quickly establishes and improves personalized predictions by allowing SwiftKey to access content on your device, including content you send through SMS, and certain apps such as Outlook.com, Gmail, Facebook and Twitter when you choose to connect them to the service.

You may also opt in to send short snippets of what and how you type for product improvement. To preserve your privacy, SwiftKey Services de-identifies these snippets, so they are not linked to your account. You can withdraw your consent to share these snippets at any time in SwiftKey Settings. You can also withdraw your consent to allow SwiftKey Services to use and retain your personal data at any time in SwiftKey Settings. When you withdraw consent, 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 and privacy in Windows, see [Windows 10 and your online services](#). 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 stored locally on your device when using different apps and features such as Microsoft Edge, some Microsoft Store apps, and Office apps. If you've signed in to your device with a Microsoft account and given 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.

Activity history is also created and sent to Microsoft when you use Microsoft apps, such as Microsoft Edge, and Office apps like Word, Excel, and PowerPoint, on mobile devices such as iOS and Android phones and tablets. If you are signed in with your Microsoft account, you can continue activities on your Windows 10 device that you started in Microsoft apps on your Android or iOS device. 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 Start > Settings > Privacy > Activity history. [Learn more about activity history in Windows 10.](#)

## 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 Settings. 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 10.](#)

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 Microsoft management tools or engages Microsoft to manage your device, we and the organization will use and process diagnostic and error data from your device to allow the management, monitoring, and troubleshooting of the organization’s devices, 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 at **Start > Settings > Privacy > 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 ensure Microsoft can troubleshoot the latest performance issue impacting users' computing experience or update a Windows 10 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 10 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 10](#).

**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 Windows 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 10.

If you choose to turn on **Tailored experiences**, we will use your Windows diagnostic data (Basic or Full as you have selected) to offer you personalized tips, ads, and recommendations to enhance Microsoft products and services for your needs. If you have selected Basic 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 Full, personalization is also based on information about the websites you browse, 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 Full.

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 don't. 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 10.](#)

## 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 is publicly viewable. Additionally, if feedback is provided using your work or school account, your feedback can be viewed through the Feedback Hub by your organization's IT administrators.

When you submit feedback to Microsoft about a problem, or upvote a problem, diagnostic data will be sent to Microsoft to improve Microsoft products and services. Depending on your Diagnostic data settings in **Start > Settings > Privacy > Diagnostics & feedback**, 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. Microsoft may also share your feedback and diagnostic data 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 10.](#)

## Location services, motion sensing, 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 copy of 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/>), to improve the location services of the provider.

Windows services and features (such as browsers and Cortana), 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 device's Settings menu.

In Settings, 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.

Even when you've turned off access to the device's location, some third-party desktop apps and services could use other technologies (such as Bluetooth, Wi-Fi, cellular modem, etc.) to determine the device's precise location. [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.](#)

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 10.](#)

**General Location.** If you turn on the General Location feature, apps that cannot use your precise location will have access to your general location, such as your city, postal code, or region.

**Find My Phone.** The Find My Phone feature allows you to find the location of your Windows phone from the [Microsoft account website](#), even if you have turned off all access to the location service on the phone. If you have turned on the "save my location every few hours" feature in the Find My Phone settings on your phone, the Find My Phone feature will periodically send and store a single last-known location of your phone, even if you have turned off location services on your phone. Each time a new location is sent, it replaces the previously-stored location.

**Find my device.** The Find my device feature allows an administrator of a Windows portable 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 10.](#)

**Windows motion sensing.** Windows devices with motion activity detection can collect motion activity. This data can enable features such as a pedometer to count the number of steps you take, so a fitness application can estimate how many calories you burn. This data and history is stored on your device and can be accessed by applications you give permission to access and use that data.

**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 includes whether you need to get consent from all parties to the communication in advance.** Microsoft is not responsible for how you use recording features or your recordings.

## 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 to understand and set boundaries on how their child is using their device. There are many features available to Family members, so please carefully review the information provided when you create or join a Family. 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 after a short period of time.

**Microsoft Defender SmartScreen.** Microsoft Defender SmartScreen helps protect you when using our services by checking downloaded files and web content for malicious software, potentially unsafe web content, and other threats to you or your device. When checking 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. If Microsoft Defender SmartScreen identifies the file as unknown or potentially unsafe, you will see a warning prior to opening the file. When checking web content, data about the content and your device is sent to Microsoft, including the full web address of the content. 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 Settings.

**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.

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 a cloud-based (online) speech recognition service, in regions where Cortana is available. To learn more about what languages and regions speech currently supports, see [Cortana's regions and languages](#).

Turning on the online speech recognition setting lets you use Microsoft's cloud-based speech recognition in Cortana, the Mixed Reality Portal, dictation in Windows from the software keyboard, supported Microsoft Store apps, and over time in other parts of 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 service.

When you use the Microsoft's cloud-based speech recognition service, Microsoft collects and uses your voice recordings to create a text transcription of the spoken words in the voice data. The voice data is used in the aggregate to help improve our ability to correctly recognize all users' speech.

You can use device-based speech recognition without sending your voice data to Microsoft. However, Microsoft's cloud-based speech recognition service provides more accurate recognition than the device-based speech recognition. When the online speech recognition setting is turned off, speech services that don't rely on the cloud and only use device-based recognition—like the Narrator app or the Windows Speech Recognition app—will still work.

If you've given permission in Cortana, we also collect additional information, like your name and nickname, your recent calendar events, and the names of the people in your appointments, information about your contacts including names and nicknames, names of your favorite places, apps you use, and information about your music preferences. This additional data enables us to better recognize people, events, places, and music when you dictate commands, messages, or documents.

You can turn off online speech recognition at any time. This will stop your voice data from being sent to Microsoft. If you are using a HoloLens or 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. To control the voice data Microsoft has associated with your Microsoft account, please visit the [Microsoft privacy dashboard](#). When you turn off the online speech recognition setting, any voice data collected while you were not signed in with a Microsoft account will be disassociated from your device. [Learn more about the online speech recognition in Windows 10](#).

**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 to "Hey Cortana."



If you've given permission for an app to listen for voice keywords, Windows 10 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.

Allowing Cortana to use voice activation and respond to "Hey Cortana" means your voice data will be collected and used in the aggregate to help improve our ability to correctly recognize all users' speech. For more information about Cortana's features and how to manage them, see [Cortana and privacy](#). Microsoft does not collect voice recordings on behalf of any third-party apps for which you have allowed voice activation.

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 10](#).

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](#).

**Inking & Typing Personalization.** Your typed and handwritten words are collected to provide you with: a personal dictionary, better character recognition to help you type and write on your device, and text suggestions that appear as you type or write. If you sync your Windows device settings to other Windows devices, your local user dictionary will be stored in your personal OneDrive for the purpose of enabling sharing of your dictionary with your other Windows devices. [Learn more about sync settings](#).

You can turn off Inking & typing personalization at any time. This will delete data stored on your device, such as your local user dictionary. [Learn more about inking & typing personalization in Windows 10](#).

## Sync settings

---

When you sign in to Windows with a Microsoft account, Windows syncs some of your settings and data with Microsoft servers to make it easier to have personalized experiences across multiple devices. After you've signed in to one or more devices with a Microsoft account, when you sign in to another with the same Microsoft account for the first time, Windows will download and apply the settings and data you choose to sync from your other devices. Settings you choose to sync will automatically update on Microsoft servers and your other devices as you use them.

Some of the settings that are synced include:

- Apps you've installed from the Microsoft Store
- Language preferences
- Ease of Access preferences
- Personalization settings such as your account picture, background, and mouse settings
- Settings for Microsoft Store apps

- Spell-checker dictionaries, input method editor (IME) dictionaries, and personal dictionaries
- Internet Explorer browser history, favorites, and websites you have open
- Saved app, website, mobile hotspot, and Wi-Fi network names and passwords

You can choose whether to sync your settings, and control what is synced, by going to **Start > Settings > Accounts > Sync your settings**. Some apps have their own, separate sync controls. If you sign in to Windows with a work account and you choose to connect that account to your personal Microsoft account, Windows will ask which settings you want to sync before connecting your Microsoft account.

## 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 Office.

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.** which 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 collect 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 settings](#) section of this privacy statement.

**Camera and Photo apps.** If you allow the Camera app to use your location, location data is embedded in the photos you take with your device. Other descriptive data, such as camera model and the date that the picture 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. You can 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.

The Photos app presents different tabs to group photos and videos by time, location, tags, and faces. The Collection tab displays photos and videos according to their time. The Album tab helps users organize their photos and videos by location and common tags. The People tab organizes photos and videos by faces.

When you import photos and videos that include location attributes, the Photos app can group your photos and videos by time and location. To do so, the Photos app sends location data in your photos and videos to Microsoft to determine the names of locations, such as "Seattle, Washington." When you sign-in to the Photos app using your Microsoft account, and you have configured your system to synchronize your local device file system with OneDrive, Photos will use object detection to tag and sort your photos and videos into Albums.

If you enable the "People" toggle on Photos Settings page, the app uses both face detection and face recognition technologies to organize your private collection into groups. Face detection is used to identify photos and videos containing faces. Face recognition groups photos and videos containing a given person's face.

You can choose to enable or disable grouping photos and videos by faces. If this feature is enabled, Photos' background processes scan your photo and video collections stored on your device for facial groupings and present the results within Photos' People tab on your device. Facial groupings are not accessible beyond the context of the device file system and are protected by the same security measures associated with all other content and data associated with a given Windows account. By enabling the People setting feature in Photos app, you consent to the use of facial grouping technology to organize your photo and video collection.

From the People tab, you can then choose to link facial groupings with your locally stored Contacts via the People Picker. You, and not Microsoft, are responsible for obtaining consent to link Contacts with your facial groupings, and you represent that you have obtained all necessary consents to link your photos and videos into groups.

Your groupings will be stored on your device for as long as you elect to keep the groupings or the photos or videos. Users will be prompted to reassert their consent after three years of non-interaction with the Photos app. At any time, users can turn off the People toggle under the Settings tab.

**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 **Settings > Ease of Access > Narrator > Get image descriptions, page titles and popular links**.

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 **Settings > Ease of Access > Narrator** 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.

## 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. You can delete your biometric verification data from within Settings.

## 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.

## Your Phone

---

The Your Phone app lets you link your Android phone with your Windows device, enabling a variety of cross-device experiences. You can use Your Phone 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; and share your phone screen on your Windows device through Your Phone's mirroring function.

To use Your Phone, the Your Phone app must be installed on your Windows device and the Your Phone Companion app must be installed on your Android phone. Upon launching the Your Phone app on your Windows device, you will be prompted to provide your mobile phone number. We use this mobile phone number solely to send you a link with information about downloading the Your Phone Companion app.

To use Your Phone, you must log into your Microsoft account on the Your Phone app on your Windows device and on the Your Phone Companion app on your Android phone. Your Android phone must be connected to Wi-Fi and your Windows device must be connected to the internet and permit Your Phone to run in the background. To use Your Phone's mirroring function, your Android phone must also have Bluetooth enabled. Your Phone also requires your Windows device to be set up with Windows Hello, as an additional security measure.

As part of providing Your Phone'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 Your Phone, and the amount of time you spent during setup.

You can unlink your Android phone from your Windows device at any time by logging in with your Microsoft account at [accounts.microsoft.com/devices](https://accounts.microsoft.com/devices) and updating the Settings on your Android phone. For detailed information, see [our support page](#).

**Text Messages.** Your Phone 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) but not messages sent via RCS (Rich Communication Services). To provide this functionality, Your Phone 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.** Your Phone allows you to make and receive calls from your Android phone on your Windows device. Through Your Phone, 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 Your Phone 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.** Your Phone allows you to copy, share or edit 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.** Your Phone allows you to view your Android phone's notifications on your Windows device. Through Your Phone, 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 Your Phone 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 Your Phone Settings page on your Windows device and your Android phone's settings. For detailed information, see [our support page](#).

**Mirroring.** Your Phone 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 Your Phone will play through your Android phone.

**Text-to-voice.** Your Phone 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.

## Entertainment and related services

---

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

### Xbox and Xbox Live

---

Xbox consoles are hardware devices that you can use to access and play games, movies, music, and other forms of digital entertainment. Xbox Live is the online gaming and entertainment service from Microsoft that enables you to find content and connect with friends, on Xbox Live and other gaming and social networks, from a variety of devices, including Xbox consoles, PCs and mobile devices.

When you access an Xbox experience from a device, we assign you a unique device identifier. When your Xbox console is connected to the internet, we identify which console and which version of the Xbox operating system you are currently using. When you sign up for Xbox Live, we assign an Xbox user ID and a gamertag (a nickname) to identify you. Data we collect about your use of Xbox Live is stored with these unique identifier(s).

We collect data about your use of the Xbox console, Xbox App, and Xbox Live such as:

- When you sign in and sign out of Xbox Live, the games you play and apps you use, your game progress and play statistics, the purchases you make, and content you obtain.
- Performance data about Xbox consoles, Xbox App and Xbox Live, connected devices, and your network connection, including software or hardware errors.
- Content you add, upload, or share through Xbox Live, including text, images and video from within games or apps.
- Social activity, including your interactions with other gamers, and your connections, including friends and followers, on Xbox Live.
- If you use the Xbox console with Kinect, data about how you use Kinect. See below for more information about Kinect data collection.
- If you use the Xbox TV app, we collect TV viewing history from your console in a way that doesn't identify you or others.

With your consent, we will collect information about videos you purchase or view through third-party apps on your Xbox console. If you use an Xbox console that includes a storage device (hard drive or memory unit), and if you play offline or have never signed in to Xbox Live on the console, usage data will be stored on the storage device and sent to Microsoft the next time you sign in.

Microsoft uses the data we collect from your Xbox console, Xbox App, and Xbox Live to provide you with experiences, which includes securing the services and carrying out the transactions you request. In order to run our subscription services such as Game Pass, we collect certain data such as device information and game play statistics such as number of unique users and playtime per game.

We also use the data to improve and develop our products. As part of the Xbox Live service, Microsoft will also use data about you and your use of Xbox Live (such as the games you play, apps you use, subscriptions you have, purchases you make, and content you obtain) to provide you with a personalized, highly curated gaming and entertainment experience. This includes connecting you to games, content, and services, as well as presenting you with offers, discounts, and recommendations.

**Xbox Live data viewable by other users.** Your gamertag, game and play statistics, achievements, presence (whether you're currently signed in to Xbox Live), content you share, and other data about your activity on Xbox Live can be seen by other users on Xbox Live, users of third-party services you have linked your profile to, or on other properties associated with Xbox Live (including those of partner companies). For example, your gamertag and scores that show on game leaderboards are considered public and can't be hidden. For other data, like presence, you can adjust your privacy settings on the console or at [xbox.com](https://xbox.com) to limit or block sharing with the public or even with friends.

**Xbox Live data shared with game or app publishers.** When you use an Xbox Live-enabled game or any network-connected app through your Xbox console, PC or mobile device, the publisher for that game or app has access to data about your usage of Xbox Live and its game or app so it may deliver and improve its product and provide support. This data may include your Xbox user ID and gamertag, limited account information such as country and age range, data about your in game communications, enforcement activity, game-play sessions (for example, moves made in-game, types of vehicles used in-game), your presence on Xbox Live, the time you spend playing the game or app, rankings, statistics, gamer profiles, avatars or gamerpics, friends lists, activity feed, club memberships, and content that you may create or submit within the game or app. Third-party game and app publishers are independent controllers of this data and its use is subject to their privacy policies. You should carefully review their policies to determine how they will use the data. For example, publishers may choose to disclose or display game data (such as on leaderboards) through their own services. To learn more about our data-sharing practices with third-party publishers, see [Data Sharing with Games and Apps](#).

**Linking your Xbox Live profile to non-Microsoft accounts.** Some games or apps available through Xbox Live, and some social features of Xbox Live, are delivered by third-party publishers or partner companies, which may require that you create a non-Microsoft account and sign-in credentials to use that game, app, or feature. If you choose to link your Xbox Live profile with an account of a third-party publisher or partner company, we will share with them limited account and profile information but will not include any credit card or other payment information.

**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 and to navigate through the service. For example:

- If you choose, the camera can be used to sign you in to the service automatically using facial recognition. To do this, it takes an image of your face and measures distances between key points to create and store a numeric value that represents only you. 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 gameplay, Kinect will map distances between your body's joints to create a stick figure representation of you that helps Kinect enable gameplay. If you are playing online, we collect those numeric values to enable and improve gameplay and the gaming experience. Kinect also detects specific hand gestures intended to do simple system interactions (such as menu navigation, pan/zoom, and scroll).
- For some fitness games, Xbox can use the Kinect sensor to estimate your exercise data, including estimates such as your heart rate during a certain activity or the number of calories burned during a workout.
- Kinect's microphones enable voice chat between players during gameplay. They also enable voice commands for control of the console, game, or app, or to enter search terms. See below for additional details on voice data collection.
- The Kinect sensor can also be used for audio and video communications through services such as Skype.

To learn more about Kinect, for Xbox 360, see [Kinect and Xbox 360 privacy](#). For Xbox One, see [Kinect and Xbox One Privacy](#).

**Captioning.** During Xbox Live real-time chat, players may activate a voice-to-text feature, which allows the user to view the audio in-game chat as text. If a user activates this feature, the other players will have no additional notice. Microsoft uses this data to provide captioning of chat for users who need it as well as the other purposes described in this privacy statement.

**Communications monitoring.** Xbox Live includes communications features such as text and voice direct messaging and real-time text and voice chat. In order to help provide a safe gaming environment and enforce the [Microsoft Code of Conduct](#), we collect and monitor direct messaging, and text communications in live-hosted multiplayer gameplay sessions and other features of the service, such as activity feeds and clubs.

**Voice data for service improvement.** We collect and use for service improvement voice search requests or samples of voice commands occurring while using Kinect or Cortana. This data is stored separately from your Xbox profile.

**GameDVR.** Any player in a multiplayer game session can use GameDVR to record their view of the gameplay taking place in that session. The recording can capture your in-game character and gamertag in the game clips created by other players in the gameplay session. Note that if a player uses GameDVR on a PC, audio chat may also be captured in a game clip.

**Children and online safety.** If you have children or teenagers who use Xbox Live, you can set up child and teen profiles for them. Children and teens under 18 cannot create a profile on Xbox Live without parental consent. Adults in the family can change consent choices and online safety settings for child and teen profiles on [xbox.com](#).

## 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 Office, 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**, 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, Microsoft Store will automatically check for, download, and install app updates to ensure 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.

MSN

---

MSN services include websites and a suite of apps, including MSN News, Weather, Sports, and Money, and previous versions of the apps branded as Bing (together, "MSN Apps"). The MSN Apps are available on various platforms, including Windows, iOS, and Android. MSN



services are also included within other Microsoft services, including the Microsoft Edge browser.

When you install MSN Apps, 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 MSN App users and identify performance issues associated with different app versions, operating systems, and browsers.

We also collect data about how you interact with MSN services, such as usage frequency and articles viewed, to provide you with relevant content. Some MSN services provide 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 MSN and Bing settings, as well as through settings in other Microsoft services that include MSN 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 MSN 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.

## Mixer

---

Mixer is an interactive, social, public online service for live streaming videos, videogames, and related content. Mixer collects account data, the information you provide for your public profile, content (such as chat and streams), and device and service usage data to provide the service, including the third-party experiences you choose, improve our products, communicate with you, and show you advertising. Your interactions with the service and with other users on the service are public and viewable by anyone, including chatting, following and subscribing to channels, and interacting with streamers, users, videos, and games. Additionally, if you chat or stream content on the service, any personal information you include will be public and may be captured and shared by others. Note that Microsoft may review and reject any content you stream or store on the service for violations of the Mixer [Rules of User Conduct](#).

Some of the apps and experiences on Mixer are provided by third-party developers. When you choose to use third-party apps or experiences: (i) your data is subject to that third party's privacy policy; and (ii) with your consent, the third party developer will have access to information about you that is not part of your public profile, such as your settings, email address and age range.

## 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.

- [Sitemap](#)
- [Contact Microsoft](#)
- [Privacy & cookies](#)
- [Terms of use](#)
- [Trademarks](#)
- [Safety & eco](#)
- [About our ads](#)
- © Microsoft 2020