

# Microsoft Privacy Statement

Last Updated: August 2016 [What's new?](#)

Microsoft participates in the EU-U.S. Privacy Shield framework. To learn more visit <https://go.microsoft.com/fwlink/?LinkID=822639>.

Your privacy is important to us. This privacy statement explains what personal data we collect from you and how we use it. We encourage you to read the summaries below and to click on "Learn More" if you'd like more information on a particular topic.

The product-specific details sections provide additional information relevant to particular Microsoft products. This statement applies to the Microsoft products listed below, as well as other Microsoft products that display this statement. References to Microsoft products in this statement include Microsoft services, websites, apps, software and devices.

## Personal Data We Collect

---

Microsoft collects data to operate effectively and provide you the best experiences with our products. You provide some of this data directly, such as when you create a Microsoft account, submit a search query to Bing, 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 recording how you interact with our products by, for example, using technologies like [cookies](#), and receiving error reports or usage data from software running on your device.

We also obtain data from third parties. For example, we supplement the data we collect by purchasing demographic data from other companies. We also use services from other companies to help us determine a location based on your IP address in order to customize certain products to your location.

You have choices about the data we collect. When you are asked to provide personal data, you may decline. But if you choose not to provide data that is necessary to provide a product or feature, you may not be able to use that product or feature.

The data we collect depends on the products and features you use, and can include the following:

**Name and contact data.** We collect your first and last name, email address, postal address, phone number, and other similar contact data.

**Credentials.** We collect passwords, password hints, and similar security information used for authentication and account access.

**Demographic data.** We collect data about you such as your age, gender, country, and preferred language.

**Payment data.** We collect data necessary to process your payment if you make purchases, such as your payment instrument number (such as a credit card number), and the security code associated with your payment instrument.

**Usage data.** We collect data about how you and your device interact with Microsoft and our products. For example, we collect:

- *Product use data.* We collect data about the features you use, the items you purchase, and the web pages you visit. This data includes your voice and text interactions with Bing, Cortana, and our chat bots.
- *Device data.* We collect data about your device and the network you use to connect to our products. It includes data about the operating systems and other software installed on your device, including product keys. It also includes IP address, device identifiers (such as the IMEI number for phones), regional and language settings.
- *Error reports and performance data.* We collect data about the performance of the products and any problems you experience with them. This data helps us to diagnose problems in the products you use, and to improve our products and provide solutions. Depending on your product and settings, error reports can include data such as the type or severity of the problem, details of the software or hardware related to an error, contents of files you were using when an error occurred, and data about other software on your device.
- *Support Data.* When you engage Microsoft for support, we collect data about you and your hardware, software, and other details related to the support incident. Such data includes contact or authentication data, the content of your chats and other communications with Microsoft support, data about the condition of the machine and the application when the fault occurred and during diagnostics, and system and registry data about software installations and hardware configurations.

**Interests and favorites.** We collect data about your interests and favorites, such as the teams you follow in a sports app, the stocks you track in a finance app, or the favorite cities you add to a weather app. In addition to those you explicitly provide, your interests and favorites may also be inferred or derived from other data we collect.

**Contacts and relationships.** We collect data about your contacts and relationships if you use a Microsoft product to manage contacts, or to communicate or interact with other people or organizations.

**Location data.** We collect data about your location, which can be either precise or imprecise. Precise location data can be Global Position System (GPS) data, as well as data identifying nearby cell towers and Wi-Fi hotspots, we collect when you enable location-based products or features. Imprecise location data includes, for example, a location derived from your IP address or data that indicates where you are located with less precision, such as at a city or postal code level.

**Content.** We collect content of your files and communications when necessary to provide you with the products you use. For example, if you receive an email using Outlook.com or Exchange Online, 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. Examples of this data include: the content of your documents, photos, music, or videos you upload to a Microsoft service such as OneDrive, as well as the content of your communications sent or received using Microsoft products such Outlook.com or Skype, including the:

- subject line and body of an email,
- text or other content of an instant message,
- audio and video recording of a video message, and
- audio recording and transcript of a voice message you receive or a text message you dictate.

We also collect the content of messages you send to us, such as feedback and product reviews you write, or questions and information you provide for customer support. When you contact us, such as for customer support, phone conversations or chat sessions with our representatives may be monitored and recorded. If you enter our retail stores or other facilities, your image may be captured by our security cameras.

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 for three basic purposes, described in more detail below: (1) to operate our business and provide (including improving and personalizing) the products we offer, (2) to send communications, including promotional communications, and (3) for some products, to show advertising.

In carrying out these purposes, we combine data we collect to give you a more seamless, consistent and personalized experience. For example, [Cortana](#) can use the favorite sports teams you add to the [MSN Sports](#) app to provide information relevant to your interests, or [Windows Store](#) can use information about the apps and services you use to make personalized app recommendations. However, to enhance privacy, we have built in technological and procedural safeguards designed to prevent certain data combinations. For example, 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.

**Providing and improving our products.** We use data to provide and improve the products we offer and perform essential business operations. This includes operating the products, maintaining and improving the performance of the products, including developing new features, research, and providing customer support. Examples of such uses include the following.

- **Providing the Products.** We use data to carry out your transactions with us and to provide our products to you. Often, those products include personalized features and recommendations that enhance your productivity and enjoyment, and tailor your product experiences based on your activities, interests and location.
- **Customer support.** We use data to diagnose product problems, repair customers' devices, and provide other customer care and support services.
- **Product activation.** We use data - including device and application type, location, and unique device, application, network and subscription identifiers - to activate software and devices that require activation.
- **Product Improvement.** We use data to continually improve our products, including adding new features or capabilities, such as using error reports to improve security features, using search queries and clicks in Bing to improve the relevancy of the search results, using usage data to determine what new features to prioritize, or using audio recordings from voice input features to improve speech recognition accuracy.
- **Security, Safety and Dispute Resolution.** We use data to protect the security and safety of our products and our customers, to detect and prevent fraud, to confirm the validity of software licenses, to resolve disputes and enforce our agreements. 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, many of our communications and file syncing products 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 may block delivery of a communication or remove content if it violates our terms.

- **Business Operations.** We use data to develop aggregate analysis and business intelligence that enable us to operate, protect, make informed decisions, and report on the performance of our business.

**Communications.** We use data we collect to deliver and personalize our communications with you. For example, we may contact you by email or other means to inform you when a subscription is ending, let you know when security updates are available, remind you about items left in your online shopping cart, update you or inquire about a service or repair request, invite you to participate in a survey, or tell you that you need to take action to keep your account active. Additionally, 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 email subscriptions and promotional communications, please visit the [Access and Controls](#) section of this privacy statement.

**Advertising.** Many of our products are supported by advertising. We use the data we collect to help select some of the ads you see - whether in our own products, like MSN and Bing, or in those offered by third parties. We partner with third parties such as AOL and AppNexus to select and deliver display ads to our sites and apps, as well as other sites and apps serviced by these partners. Microsoft also delivers search ads to Bing and to other websites and services that use our search functionality. The ads we select may be based on your current location, search query, or the content you are viewing. Other ads are targeted based on your likely interests or other information that we learn about you over time using demographic data, search queries, interests and favorites, usage data from our own sites and apps and the sites and apps of our advertisers and partners, and location data - which we refer to as "interest-based advertising" in this statement. 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. **You can opt out of receiving interest-based advertising from Microsoft by visiting our [opt-out page](#).** More information about advertising controls is available in the [Access and Controls](#) section of this privacy statement. 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 interest-based 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 target ads based on custom, non-sensitive health-related interest categories as requested by advertisers.
- **Children and Advertising.** We do not deliver interest-based advertising to children whose birthdate in their Microsoft account identifies them as under 13 years of age.
- **Data Retention.** For interest-based 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. Advertisers may choose to place our [web beacons](#) on their sites 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 help target their ads. We also share data directly with service providers (such as AOL and AppNexus) to permit them to provide services on our behalf or to partner with us in selecting and serving ads for our advertising partners.
- **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: [A9](#), [AOL Advertising](#), [AppNexus](#), [Criteo](#), [Facebook](#), [MediaMath](#), [nugg.adAG](#), [Rocket Fuel](#), [Yahoo!](#). You may find more information on each company's practices, including the choices it offers, by clicking on the company names above. Many of them are also members of the [NAI](#) or [DAA](#), which each provide a simple way to opt out of ad targeting from participating companies.

## 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. 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 in order 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 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:

1. comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies;
2. 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;
3. operate and maintain the security of our products, including to prevent or stop an attack on our computer systems or networks; or
4. 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 Transparency Report, available at <http://microsoft.com/about/corporatecitizenship/en-us/reporting/transparency>.

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

## How to Access & Control Your Personal Data

---

You can view or edit your personal data online for many Microsoft products. You can also make choices about Microsoft's collection and use of your data. How you can access or control your personal data will depend on which products you use. For example:

- **Microsoft account.** If you wish to access or edit 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 <https://account.microsoft.com>. From here, you can also access controls for other Microsoft products.
- **Bing and Cortana.** You can access or clear your Bing search history, redeem Bing Rewards, view and modify interests, and manage other Cortana data at <https://www.bing.com/account/general>.
- **Skype.** If you wish to access or edit the profile information and payment information in your Skype account or change your password, you can sign into your account at <https://login.skype.com/login>.
- **Xbox.** If you use Xbox Live or Xbox.com, you can view or edit your personal data, including billing and account information, privacy settings, 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 <https://www.microsoftstore.com/> and clicking on "View account" or "Order history."
- **Microsoft.com.** You can access and update your profile on microsoft.com by visiting the [Microsoft.com Profile Center](#). If you have a Microsoft Developer Network public profile, you can access and edit it at <https://connect.microsoft.com/profile.aspx>.

If you cannot access certain personal data collected by Microsoft via the links above or directly through the Microsoft products you use, you can always contact Microsoft by using our [web form](#). We will respond to requests to access or delete 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 visiting and signing into Microsoft's [Promotional Communications Manager](#) with your personal [Microsoft account](#), which allows you to 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 services, or to surveys or other informational communications that have their own unsubscribe method.

## Your Advertising Choices

You may opt out of receiving interest-based advertising from Microsoft by visiting our [opt-out page](#). When you opt out, your selection will be 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 will 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 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 necessary purposes (including providing our products, analytics and fraud detection), opting out of interest-based advertising does not stop that data from being collected. Nor does it mean you will stop getting ads or see fewer ads. However, if you do opt out, the ads you receive will no longer be interest-based and may be less relevant to your interests.

## Browser-Based Controls

- **Cookie Controls.** Relevant browser-based cookie controls are described in the [Cookies](#) section of this privacy statement.
- **Tracking Protection.** Internet Explorer (versions 9 and up) has a feature called Tracking Protection that will block third-party content, including cookies, from any site that is listed in a Tracking Protection List you add. By limiting calls to these sites, the browser will limit the information these third-party sites can collect about you.
- **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 & Similar Technologies

---

Microsoft uses cookies (small text files placed on your device) and similar technologies to provide our websites and online services and help collect data. The text in a cookie often consists of a string of numbers and letters that uniquely identifies your computer, but it can contain other information as well. Microsoft apps use other 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 product, including:

- **Storing your Preferences and Settings.** Settings that enable our products to operate correctly or that maintain your preferences over time may be stored on your device. For example, if you enter your city or postal code to get local news or weather information on a Microsoft website, we may store that data in a cookie so that you will see the relevant local information when you return to the site. If you opt out of interest-based advertising, we store your opt-out preference in a cookie on your device.
- **Sign-in and Authentication.** When you sign into 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.
- **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 [Access and Control](#) section of this privacy statement.
- **Analytics.** In order to provide our products, we use 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.

Some of the cookies we commonly use are listed in the following chart. This list is not exhaustive, but it is intended to illustrate the main reasons we typically set cookies. If you visit one of our websites, the site may set some or all of the following cookies:

Cookie name	Description
MUID	Identifies unique web browsers visiting Microsoft sites. It is 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.
RPSTAuth, MSNRPSAuth, KievRPSAuth	Helps to authenticate you when you sign in with your Microsoft account.
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.
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 may also set cookies when you visit Microsoft sites. In some cases, that is because we have hired the third party to provide services on our behalf, such as site analytics. In other cases, it is because our web pages contain content or ads from third parties, such as videos, news content or ads delivered by other ad networks. Because your browser connects to those third parties' web servers to retrieve that content, those third parties are able to set or read their own cookies on your device and may collect information about your online activities across websites 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 clicking **Settings > Privacy > Cookies**. Instructions for blocking or deleting cookies in other browsers may be available in each browser's privacy or help documentation.

Certain features of Microsoft products depend on cookies. Please be aware that if you choose to block cookies, you may not be able to sign in or use those features, and preferences that are dependent on cookies may be lost. If you choose to delete cookies, settings and preferences controlled by those cookies, including advertising preferences, will be deleted and may need to be recreated.

Additional privacy controls that can impact cookies, including the Tracking Protection feature of Microsoft browsers, are described in the [Access and Control](#) section of this privacy statement.

**Our Use of Web Beacons and Analytics Services**

Microsoft web pages may contain electronic images known as web beacons (also called single-pixel gifs) 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 in our promotional email messages or newsletters 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 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.

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 the following links:

- Flurry Analytics: <http://flurry.com/legal-privacy/end-user-opt-out>
- Google Analytics: <http://tools.google.com/dlpage/gaoptout> (requires you to install a browser add-on)
- Kissmetrics: <https://kissmetrics.com/user-privacy>
- Mixpanel: <https://mixpanel.com/optout>
- Nielsen: [http://www.nielsen-online.com/corp.jsp?section=leg\\_prs&nav=1#Optoutchoices](http://www.nielsen-online.com/corp.jsp?section=leg_prs&nav=1#Optoutchoices)
- Omniture (Adobe): <http://www.d1.sc.omtrdc.net/optout.html>
- Visible Measures: <http://corp.visiblemeasures.com/viewer-settings>
- WebTrends: <https://ondemand.webtrends.com/support/optout.asp>

## 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 be used to store a unique identifier for your computer, which can then be used to track behavior. These technologies include Local Shared Objects (or "Flash cookies") and Silverlight Application Storage.

**Local Shared Objects or "Flash cookies."** Web sites that use Adobe Flash technologies can use Local Shared Objects or "Flash cookies" to store data on your computer. To manage or block Flash cookies, go to [http://www.macromedia.com/support/documentation/en/flashplayer/help/settings\\_manager.html](http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html).

**Silverlight Application Storage.** Web sites 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 statement.

## Microsoft account

---

With a Microsoft account, you can sign into Microsoft products, as well as those of select Microsoft partners. When you create your own Microsoft account, we refer to that account as a personal Microsoft account. When you sign into products that use Microsoft Azure Active Directory (AAD) with an email address from your employer or school, we refer to that account as a work or school account.

**Creating and using your personal Microsoft account.** When you create a personal Microsoft account, you will be asked for 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 into and use some 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, and your employer or school that issued that address begins managing that account with Azure Active Directory (AAD), you will need to update the email address associated with your personal Microsoft account in order to continue accessing Microsoft products that do not use AAD (such as Xbox Live).

**Signing in.** When you sign into your Microsoft account, we create a record of your sign-in, which includes the date and time, information about the product you signed into, 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 into Microsoft.** Signing into your account enables improved personalization, provides seamless and consistent

experiences across products and devices, and allows you to access and use cloud data storage and other enhanced features and settings. When you sign into 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 into products that use Microsoft account that you access 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 into third-party products.** If you sign into a third-party product with your Microsoft account, you will be asked to consent to share the account data required by that product. 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 whether your account has been deactivated. The third party can use or share your data according to its own practices and policies. If you have consented to share your profile data, the third party may display your name or username and your profile photo (if you have added one to your profile) when you are signed in to that third-party product. **You should carefully review the privacy statement for each product you sign into to determine how it will use the data it collects.**

**Personal Microsoft accounts received from third parties.** If you received your personal Microsoft account from a third party, like an Internet service provider, that third party may have rights over your account, including the ability to access or delete your Microsoft account. **You should carefully review any additional terms the third party provided you to understand what it can do with your account.**

**Connecting your personal Microsoft account to your social network accounts.** You may connect your personal Microsoft account to your accounts on social networks such as Facebook, Twitter or LinkedIn in order to access data from those social networks from within Microsoft products. If you choose to do so, we will store data about your social network accounts on our servers so that we can display updated data from your social network account. You can disconnect a social network account from your personal Microsoft account at any time at <https://profile.live.com/services>.

**Using work or school accounts.** If your employer or school uses Azure Active Directory (AAD) to issue and manage the account it provides you, you can use your work or school account to sign into Microsoft products that use AAD (such as Office 365 or Skype for Business). If required by your organization, you will also be asked to provide a phone number or an alternative email address for additional security verification. If you sign into Microsoft products with a work or school account, 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. Your use of the products may be subject to your organization's policies, if any. Microsoft is not responsible for the privacy or security practices of these organizations, which may differ from those of Microsoft. If your organization is administering your use of Microsoft products, please direct your privacy inquiries to your administrator.

## Other Important Privacy Information

---

Below you will find additional privacy information you may find important. You can also find more information on Microsoft's commitment to protecting your privacy at <https://privacy.microsoft.com>.

### 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.

### Where We Store and Process Personal Data

---

Personal data collected by Microsoft may be stored and processed in your region, in the United States or in any other country where Microsoft or its affiliates, subsidiaries or service providers maintain facilities. 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.

When we transfer personal data from the European Economic Area to other countries, we use a variety of legal mechanisms, including contracts, to help ensure your rights and protections travel with your data. Microsoft adheres to the principles of the U.S.-Swiss Safe Harbor framework, and intends to adopt the forthcoming EU-U.S. Privacy Shield Principles, regarding the collection, use, and retention of data from the European Economic Area and Switzerland. To learn more about the Safe Harbor program, and to view our certification, please visit <http://www.export.gov/safeharbor>.



Microsoft retains personal data for as long as necessary to provide the products and fulfill the transactions you have requested, or for other essential purposes such as complying with our legal obligations, resolving disputes, and enforcing our agreements. 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 after 18 months.
- In Outlook.com, when your Deleted Items folder is emptied, those emptied items remain in our system for up to 30 days before final deletion.
- If you remove a credit card from your account, Microsoft will retain transaction records containing your credit card number for as long as reasonably necessary to complete any existing transactions, to comply with Microsoft's legal and reporting requirements, and for the detection and prevention of fraud.

## Collection of Data From Children

---

When a Microsoft product collects age it will either block users under 13 or will ask them to provide consent from a parent or guardian before they can use it. We will not knowingly ask children under 13 to provide more data than is necessary to provide the product.

Once parental consent is granted, the child's account is treated much like any other account. The child may have access to communication services like email, instant messaging and online message boards and may be able to communicate freely with other users of all ages.

Parents can change or revoke the consent choices previously made, and review, edit or request the deletion of their children's personal data. For example, parents can access their personal [Microsoft account](#) and click on "Permissions." For users of Minecraft and other Mojang games, parents can contact us at <https://account.mojang.com/terms#contact>.

## Preview Releases

---

Microsoft offers preview, insider, beta or other pre-release products and features ("previews") to enable you to evaluate them while providing feedback, including performance and usage data, to Microsoft. 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 will update this privacy statement when necessary to reflect customer feedback and changes in our products. When we post changes to this statement, we will revise the "last updated" date at the top of the statement and describe the changes in the [Change History](#) page. If there are material changes to the statement or in how Microsoft will use your personal data, 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 technical or support question, please visit <http://support.microsoft.com> to learn more about Microsoft Support offerings. If you have a personal Microsoft account password question, please visit [Microsoft account support](#).

If you have a privacy concern or a question for the Chief Privacy Officer of Microsoft, please contact us by using our [Web form](#). We will respond to questions or concerns within 30 days.

Unless otherwise stated, Microsoft Corporation is a data controller for personal data we collect through the products subject to this statement. Our address is Microsoft Privacy, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, USA. Telephone: (+1) 425-882-8080.

Microsoft Ireland Operations Limited is our data protection representative for the European Economic Area and Switzerland. The data protection officer of Microsoft Ireland Operations Limited can be reached at the following address: Microsoft Ireland Operations, Ltd., Attn: Data Protection, Carmenhall Road, Sandyford, Dublin 18, Ireland.

To find the Microsoft subsidiary in your country or region, see <http://www.microsoft.com/worldwide/>.

## Bing

---

Bing services include search and mapping services, as well as the Bing Toolbar and Bing Desktop apps. Bing services are also included within other Microsoft services, such as [MSN Apps](#) and [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 search or command terms you provide, along with your IP address, location, the unique identifiers contained in our [cookies](#), the time and date of your search, and your browser configuration. If you use Bing voice-enabled services, additionally your voice input and performance data associated with the speech functionality 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 web page 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 to conduct a search will be sent to Microsoft. This allows us to provide you with suggestions as you type your searches. To turn this feature on or off, go to [Bing settings](#).

**Bing Rewards Program.** When you are signed in with your Microsoft account, we use data about your interactions with Bing services to provide rewards credits. To opt out of this feature, go [here](#).

**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 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 the [Bing Settings](#) page to manage your personalization settings.

**Managing Search History.** Bing's Search History service provides an easy way to revisit the search terms you've entered and results you've clicked when using Bing search through your browser. You may clear your search history in [Bing Settings](#). Clearing your history removes it from the Search History service and prevents that history from being displayed on the site, but does not delete information from our search logs, which are retained and de-identified as described above.

**Non-Microsoft services that use Bing.** You may access Bing-powered experiences when using other non-Microsoft services, such as those from Yahoo!. In order to provide these services, Bing receives data from these and other partners that may include date, time, IP address, a unique identifier and other search-related data. This data will be sent to Microsoft in order 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 non-Microsoft services for any questions about how they collect and use data.

**Search query passed in referral URL.** When you click on 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](#) that page sets.

**Sharing search data for research and development purposes.** We share some de-identified search query data with selected third parties for research and development purposes. Before we do so, we remove all unique identifiers such as IP addresses and cookie IDs from the data. We also 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 other purposes.

## Cortana

---

Cortana is your personal assistant. Cortana works best when you sign in and let her use data from your device, your personal Microsoft account, other Microsoft services, and third-party services you choose to connect. If you choose not to sign into Cortana, you can still chat with Cortana and use Cortana to help you search the web and your device. But if you don't sign in, your experiences will be more limited and they will not be personalized.

**Signed out.** When you are not signed in, Cortana will collect data about how you chat with Cortana and use Cortana to search, using either your voice, inking, or typing. This data includes the following:

- **Speech, inking, and typing.** To help Cortana better understand the way you speak and your voice commands, speech data is sent to Microsoft to build speech models and improve speech recognition and user intent understanding. If you choose to sign in, the speech models will become more personalized.
- **Search history.** Your Bing search queries - 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.
- **Device Data.** Cortana can access data about your device and how you use it. For instance, it can determine if Bluetooth is on, whether your lock screen is on, your alarm settings, and which apps you install and use.

**Signed in.** If you sign in, you enable Cortana to perform additional tasks and to provide personalized experiences and relevant suggestions; and you give Cortana permission to collect or access the following additional types of data:

- **Microsoft account.** Cortana can access the demographic data (such as your age, postal code and gender) you provided when you created your personal [Microsoft account](#).
- **Other Microsoft product usage.** Cortana uses data collected through other Microsoft services to provide personalized suggestions. For example, Cortana uses data collected by the MSN Sports app so it can automatically display information about the teams you follow. It also learns your favorite places from Microsoft's Maps app, your favorite songs and artists from the music you play in [Groove Music](#), and what you view and purchase in the [Windows Store](#) so it can offer better suggestions. Your interests in Cortana's 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.

**Location.** You can choose whether Cortana accesses your location information in order to give you the most relevant notices and results and to make suggestions that help save you time, such as 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).

**Contacts, email, calendar & communications.** You can choose to let Cortana access your email and other communications, your calendar, and your contacts in order to enable additional features and personalization. If you give permission, Cortana will access additional data including:

- **Text messages and email.** Cortana accesses your messages to do a variety of things such as: allowing you to add events to your calendar, apprising you of important messages, and keeping you up to date on events or other things that are important to you, like package or flight tracking. Cortana also uses your messages to help you with planning around your events and offers other helpful suggestions and recommendations.
- **Communications History.** Cortana learns who is most important to you from your call, text message, and email history. This data is used to keep track of people most relevant to you and your preferred methods of communication, flag important messages for you (such as missed calls), and improve the performance of Cortana features such as speech recognition.
- **Calendar appointments.** Cortana access your calendars in order to provide reminders and information relevant to your appointments.

**Browsing history.** If you allow Cortana to use your Microsoft Edge browsing history (see the [Microsoft Edge](#) description in the Windows section of this statement), Cortana can help you pick up where you left off on websites, and provide suggestions based on the sites you visit in Microsoft Edge. Cortana won't collect information about sites you visit in InPrivate tabs.

**Other Connected Services.** You can also give Cortana access to other data collected by other Microsoft and third party services by connecting those services with Cortana.

- **Connected Microsoft services.** If you choose to connect Cortana to your [Xbox Live](#) account, Cortana can access your Xbox Live data in order to learn about your gaming activity and provide you with relevant content and suggestions, notify you when your friends are available to play, and help you schedule game sessions. If you choose to connect Cortana to your [Office 365](#) work or school account, Cortana can access data stored in Office 365 to help you stay up to date and get insights about your meetings, documents, and relationships.
- **Connected third-party services.** Cortana allows you to connect to third-party services to enable her to do more and provide additional personalized experiences based upon data from the third-party service, such as LinkedIn or Uber. For example, choosing to sign into LinkedIn within Cortana allows Microsoft to access your LinkedIn data so that Cortana can give you more personalized information and recommendations. ***When Cortana is connected to a third-party service, it can also send data to that service to enable the connected service.*** For instance, Cortana will send to LinkedIn the name, email address, job title, and company name of people you are meeting with, in order for Cortana to retrieve relevant information about those contacts. Similarly, Cortana will send your current location and destination to Uber when you ask Cortana to request a ride. You can manage Cortana's connections to third-party services in the Cortana Notebook.

Remember that you can always sign out of Cortana, and when you do, Cortana will still be there to help, but your experiences will not be personalized. You can manage what data Cortana uses, and what it knows about you in Cortana Settings, Permissions, and Notebook. More about the individual features, and how to manage them can be found at <http://go.microsoft.com/fwlink/?linkid=522360>.

## Groove Music/Movies & TV

---

Groove Music lets you easily play your music collection, make playlists, buy music and stream custom radio stations. 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. If you enable Cortana on your device, Microsoft will collect and use data related to the music you play via Groove Music to provide personalized experiences and relevant suggestions.

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 Groove Music or 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.

## Microsoft Health Services

---

Microsoft Health services can help you understand and manage your health data. They include the Microsoft Band devices, Microsoft Health apps, HealthVault, and other related services. The Band helps you keep track of data like heart rate and steps taken. The Band can also use Cortana to take notes and receive notifications from your phone. The Microsoft Health app sends data to Microsoft's servers and allows you to manage and control the data. The app provides a channel for other apps on your phone to send notifications to the Band. HealthVault is a personal health platform that lets you gather, edit, add to, and store health data online. With HealthVault, you can also choose to share your health data with family, caregivers, and health care professionals.

Microsoft Health services collect and use your data to provide the services, which includes improving and personalizing your experiences. Health data you provide to Microsoft through Microsoft Health services is not combined with data from other Microsoft services, or used for other purposes without your explicit consent. For example, Microsoft does not use your health record data to market or advertise to you without your opt-in consent.

### Microsoft Health and Microsoft Band

---

Microsoft Health and Microsoft Band can help you understand and manage your health data. The data collected depends on the services and features you use, and includes the following:

- **Profile Data.** When you create a profile, you will need to provide data, such as height, weight, and age that is



used to calculate your activity results. Other profile data comes from your personal [Microsoft account](#).

- **Activity and Fitness Data.** Microsoft Band helps you keep track of your activity and fitness by collecting data like your heart rate, steps, calories burned, and sleep. Examples of types of activities you can choose to track are runs, workouts, and sleep.
- **Usage Data.** To provide you the best service, we collect and automatically upload statistics about the performance and your use of the Microsoft Health and Microsoft Band.
- **Location.** Microsoft Band has built-in Global Positioning System (GPS) capabilities, which let you map your activities like running or biking, without having to carry your phone with you. If you enable GPS for an activity, you can view the activity map in the Microsoft Health app. Some modes on the Band, such as Golf and Explorer, automatically turn on GPS, and turn it off when you end the mode.

To learn more about the Band's sensors and the data they collect, go [here](#).

**Access and Control.** You can view and manage your data in Microsoft Health. For example, in Microsoft Health, you can view and update your profile data, manage connected applications, and view past activities. You can delete specific activity details in the Microsoft Health app. When you delete a specific activity, the event is deleted from the Microsoft Health service; however, the basic sensor data captured by the devices remain in the Microsoft Health service. You can cancel your Microsoft Health account at any time by contacting Customer Support [here](#).

**Cortana.** The Band allows you to take notes, perform queries, and set reminders with your voice, if [Cortana](#) is enabled on your phone. To learn more about how [Cortana](#) manages your data, see the Cortana section of this privacy statement.

## HealthVault

---

HealthVault is a personal health platform that lets you gather, edit, store, and share health data online. With HealthVault, you can control your own health records. You can also choose to share your health data with family, caregivers, health care professionals, mobile apps, health-related devices, and online tools. For more information about HealthVault, go to [here](#).

**Signing into HealthVault.** To sign into HealthVault, you can use [Microsoft account](#) or a third-party authentication service. If you close your Microsoft account or lose your account credentials, you may not be able to access your data. You can use more than one credential with HealthVault to help ensure continued access. Before using a third-party authentication service with HealthVault, we recommend you review the security and privacy commitments offered by the issuer.

**HealthVault Account and Health Records.** To create a new HealthVault account, you must provide personal data such as name, date of birth, e-mail address, postal code and country/region. Depending on which features you use, you may be asked for additional information. A HealthVault account allows you to manage one or more health records, such as the ones you create for yourself and your family members. You can add or remove data to a health record you manage at any time.

In the U.S., HealthVault assigns each health record an email address. When a message is received at that email address, the message and attachments are automatically added to the HealthVault record, and a notification email is sent to the custodians of that record. The email service in HealthVault uses "Direct," a protocol designed specifically to communicate with health care providers. For that reason, HealthVault email can only be sent and received with providers that use a system that uses the Direct protocol. Custodians can add or disable record email addresses.

**Sharing Health Data.** A key value of HealthVault is the ability you have to share your health data with people and services that can help you meet your health-related goals. By default, you are the custodian of any records you create. Custodians have the highest level of access to a health record. As a custodian, you can share data in a health record with another person by sending an e-mail invitation through HealthVault. You can specify what type of access they have (including custodian access), how long they have access, and whether they can modify the data in the record. When you grant someone access, that person can grant the same level of access to someone else (for example, someone with view-only access can grant another user view-only access). **Because inappropriate granting of access could allow someone to violate your privacy or even revoke your access to your own records, you should be cautious about granting access to your records.**

You can choose to share specific data (or all of the data) in a health record with other services. No service has access to your data through HealthVault unless an authorized user grants it access through HealthVault. HealthVault allows you to control access by accepting or denying requests. For each service granted access, you choose what health information in a specific health record to share and what actions each service may perform on the health information.



A service you authorize for a record will get the full name associated with your HealthVault account, the nickname of the authorized record(s), and your relationship to that record. The service will continue to have access through HealthVault until you revoke the permission. Microsoft can revoke a service's access to HealthVault if it does not meet its privacy commitments to Microsoft. However, except for restricting the access they have to your HealthVault data, we do not control or monitor those services, and their privacy practices will vary.

**Reports to U.S. Health Care Providers.** In the United States, we enable participating health care providers to obtain reports about whether the information they send to a record is used. This feature supports the "meaningful use" objective of the HITECH Act, which provides incentives for health care providers to send their patients copies of their medical information electronically. Providers that participate can get reports that include a number the provider uses to identify the patient within its system, and whether the user took one of the "qualifying actions" in HealthVault (but no information about which action). "Qualifying action" currently includes activities such as viewing, downloading, or transmitting health information via email. You can turn off reporting for your records.

**Access and controls.** You can review, edit or delete your HealthVault account data, or close your HealthVault account at any time. Only custodians can permanently delete an item. When you delete a health record, it is deleted from all users who had access to it.

When you close your HealthVault account, we delete all records for which you are the sole custodian. If you share custodian access for a record, you can decide whether to delete the record. Microsoft will wait a limited amount of time before permanently deleting your data in order to help avoid accidental or malicious removal of your health data.

HealthVault maintains a full history of each access, change or deletion by users and services, which includes the date, action and name of the person or service. Custodians of records can examine the history of those records.

**Email Communications.** We will use the email address you provide when you create your HealthVault account to send you an email requesting that you validate your email address, to include in sharing invitations you send through HealthVault, and to send you service notifications, such as email notifications that information is available to add to your HealthVault records.

HealthVault periodically sends newsletters to help keep you informed of the latest improvements. HealthVault will also periodically send you an email summarizing recent account activity. Subject to your contact preferences, we also use your email addresses to send you promotional email. You can unsubscribe from these emails at any time.

## 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 content viewed. 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 Microsoft's [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 log-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.

## Office

---

Office is a collection of productivity applications including Word, Excel, PowerPoint, and Outlook among others. For more details about Outlook, see the [Outlook](#) section of this privacy statement. Various Office applications enable you to use content and functionality from other Microsoft and third-party connected services such as Bing. For detailed information about how to manage

your privacy options, please see <http://go.microsoft.com/fwlink/?LinkId=624445>. If you work in an organization, your administrator can turn off connected services via Group Policy.

**Office Roaming Service.** The Office Roaming Service helps keep your Office settings up-to-date across your devices running Office. When you sign into Office with your [Microsoft account](#), the Office Roaming 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 into 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 into 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 the [Microsoft Update](#) service to provide you with security and other important updates. See the Update Services section of this privacy statement for more information.

**Online Help, templates, fonts, and other content.** Office uses other Microsoft or third-party services to give you the latest online content when you are connected to the Internet such as Help articles, templates, and fonts. For example, when you use the Help feature in Office applications, Office sends your search query to Office.com to provide you with online Help articles. These features are turned on by default, but you can turn them off using privacy settings. You can access privacy settings in Office 2013 by clicking **File > Options > Trust Center > Trust Center Settings > Privacy Options**.

**Click-to-Run Update Service.** The Click-to-Run Update Service allows you to install certain Microsoft Office products over the Internet so you can start using them before they are completely downloaded. By default, 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. The service is turned on by default, but you can turn it off by using privacy settings.

**Search services.** Office-supported search services such as Insights allow you to request information from Microsoft or third-party services from within an Office application. For example, in Word, you can highlight a word or phrase and retrieve relevant information from Bing search. When you search on a particular word or phrase, Office sends to the service the encrypted text you requested (and when using Insights, in order to provide you with contextually relevant search results, Office will send your requested word or phrase and some surrounding content from your document). In Excel, you can send categories of data to Microsoft in order to receive recommendations for other sets of similar data that might interest you, but the actual content from your workbook isn't sent to Microsoft. In addition, Office will send data about the software you're using and the locale to which your system is set. If required by a third-party content provider, it will also send authorization data indicating you have the right to download the relevant content. Frequently, the information you receive includes a link to additional information from the content provider's website. If you click the link, the content provider may place a [cookie](#) on your device to identify you for future transactions.

**Translation service.** Some Office applications allow you to translate some or all of your document by using a bilingual dictionary or a machine translation. If a word or phrase you want to translate isn't in the bilingual dictionary included with your application software, the word or phrase is sent unencrypted to a Microsoft or a third-party translation service. If you choose to translate your entire document, the entire document is sent unencrypted to a Microsoft or a third-party translation service. In addition to the word or phrase you want to translate, Office sends information about the Office software you are using, including the version, operating system, and locale and language to which your system is set. For third-party translation services, Office might also send previously stored authentication information indicating that you previously signed up for access to the website.

## 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 in order 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 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 phone that you have synced with your OneDrive account, your content is either uploaded to that network or a link to that content is posted to that network. Content posted to social networks and hosted on OneDrive is accessible to anyone on that social network. To delete the content, you need to delete it from the social network 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 into 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 Microsoft's primary consumer email service, 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.

**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 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.

## 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.

## Skype

---

Skype lets you send and receive voice, video and instant message communications. This section applies to the consumer version of Skype; if you are using Skype for Business, see the [Enterprise Products](#) section of this privacy statement. Both Microsoft Corporation and Skype Communications S.à.r.l. (a wholly-owned Microsoft subsidiary based in Luxembourg) are data controllers for Skype, and references to Microsoft in this section refer to both legal entities.

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 usernames that are part of the communication.

**Skype profile.** 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 search directory. Your profile includes your username, 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. With your permission, Skype will also check your device or other address books from time to time 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 on their account page at [www.skype.com](http://www.skype.com).

**Skype marketing affiliate program.** So that more people can learn about Skype, we encourage other companies and organizations to sign up as marketing affiliates to refer people to Skype. When the people they refer do things like buy Skype Credit, we pay them. We partner with another company, Conversant Media, to operate our affiliate network. Microsoft, our network partner, and the marketing affiliates use cookies and web beacons so we can know which marketing affiliate made a successful referral and earned a payment. Microsoft doesn't control the cookies that the marketing affiliates set. For more information on the privacy practices of our network partner, visit <http://www.conversantmedia.com/legal/privacy>.

**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 a 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 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.

**Skype advertising.** Some Skype software includes interest-based advertising, so that you're more likely to see ads you'll like. In some versions of the software, you can opt out of interest-based advertising in the privacy options or account settings menu. If you sign in to Skype with a Microsoft account, you can opt out of interest-based advertising at <http://choice.microsoft.com>. If you opt out, you'll still see ads displayed in the Skype software based on your country of residence, language preference, and IP address location, but other data is not used for ad targeting.

**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 audio and/or video clips of your conversation. If you choose to record a session, the recording may include a few seconds of the call held in memory prior to your initiating the recording. The recording will be stored as part of your conversation history and may also be stored locally on your device. ***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.

## Store

---

The Store is an online service that allows you to browse, download, purchase, rate, and review applications and other digital content. It includes:

- Windows Store for apps and content for Windows devices such as phones, PCs, and tablets,
- Xbox Store for games and other apps for Xbox ONE and Xbox 360 consoles, and
- Office Store for products and apps for Office, SharePoint, Exchange, Access and Project (2013 versions or later).

We collect data about how you access and use the Store; the products you've viewed, purchased, or installed; the preferences you set for viewing apps in the 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 Store apps.** Many apps you install from the Windows 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 the Store. Many of the features that Windows 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 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 Store settings, the 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 the Windows 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 the Windows 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 the 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 the 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.

## SwiftKey

---

SwiftKey Keyboard and related apps and services use data about how you type – including the emoji you use and the words that matter to you – to learn your writing style and provide personalized autocorrect and predictive text that adapts to you.

When you use our products, we collect data such as device, network, performance, and usage statistics. We use this data to operate and improve the products.

If you opt in to SwiftKey Cloud, we will collect your email address, basic demographic data, and data about the words and phrases you use to enable services such as personalization, prediction synchronization, and backup. Our 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, and reflects your unique writing style. To do this, the SwiftKey Keyboard for Android accesses your SMS messages upon first installation. The SwiftKey personalization service, which is a feature of SwiftKey Cloud, also accesses your recent content from online services that you specify, such as Gmail, Facebook and Twitter. If you are logged into SwiftKey Cloud, this data will be transferred over encrypted channels to our servers. Where a field has been flagged by a website or app as denoting a password field or payment data, SwiftKey does not log, store, or learn from this data.

If you are not logged into SwiftKey Cloud, language insights will not be collected from your device. You may at any time withdraw your consent for our use and retention of personal data collected by SwiftKey by going to the SwiftKey Cloud section in SwiftKey Settings. By withdrawing consent, your personal data collected through your use of the SwiftKey Keyboard 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 in our products at any time by going to 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 control device settings, device policies, software updates, data collection by us or the organization, or other aspects of your device. For more information about data collection and privacy in Windows, go to <http://go.microsoft.com/fwlink/?LinkId=529552>. Legacy versions of Windows (including Vista, 7, 8, and 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.

### Advertising ID

---

Windows generates a unique advertising ID for each user on a device. When the advertising ID is enabled, 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 the advertising networks they work with) to provide more relevant advertising and other personalized experiences across their apps. You can turn off access to this identifier at any time in the device 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. For more information on Microsoft's use of data for advertising, see the [How We Use Data](#) section of this statement.

**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, location is determined using satellite global positioning service (GPS), detecting nearby cell towers and/or Wi-Fi access points and comparing that information against a database that Microsoft maintains of cell towers and Wi-Fi access points whose location is known, or deriving location from your IP address. When the location service is active on a Windows device, 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. Microsoft may also share this de-identified location data with third parties to provide and improve location and mapping services.

Windows services and features (such as browsers and Cortana), applications running on Windows, and websites opened in Windows browsers can access the Windows location service to determine precise location if you allow them to do so. Some features and apps request precise location permission when you first install Windows, some ask the first time you use the app, and others ask every time you access the location service. For information about certain Windows apps that use the location service, see the [Windows Apps](#) section below.

When the location service is accessed, your Windows device will also upload its location to Microsoft, and we will retain only the last known location (each new location replaces the previous one) to improve the efficiency and operation of our services. Data about a Windows device's recent location history is stored on the device, 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 applications have access to the location service or your device's location history, turn off or on access to the location service for particular applications, or turn off the location service. 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.

Note that on mobile devices, your mobile operator will have access to your location even if you turn off the location service.

**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 <https://account.microsoft.com>, 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 PC or tablet to find the location of that device if the administrator has enabled the location service for the device, even if other users have disabled location for themselves. When the administrator attempts to locate the device, users will see a notification in the notification center.

**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. **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 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.

**SmartScreen.** 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, and the file's digital certificates. If 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 is sent to Microsoft, including the full web address of the content. If SmartScreen detects that content is potentially unsafe, you will see a warning in place of the content. SmartScreen can be turned on or off in Settings.

**Windows Defender.** Windows Defender looks for malware and other unwanted software on your device. Windows Defender is automatically turned on to help protect your device if no other antimalware software is actively protecting your device. If Windows Defender is turned on, it will monitor the security status of your device. When Windows Defender 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, and it may also send files that could contain 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 Windows Defender not to send reports and suspected malware to Microsoft.

## Speech, Inking and Typing

---

Microsoft collects and uses data about your speech, inking (handwriting), and typing on Windows devices to help improve and personalize our ability to correctly recognize your input. This feature is also known as Getting to Know You.

For example, to provide personalized speech recognition, we collect your voice input. If you've given permission in Cortana, we also collect 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.

Additionally, your typed and handwritten words are collected to provide you a personalized user dictionary, help you type and write on your device with better character recognition, and provide you with text suggestions as you type or write. Typing data includes a sample of characters and words you type, which we scrub to remove IDs, IP addresses, and other potential identifiers. It also includes associated performance data, such as changes you manually make to text as well as words you've added to the dictionary.

You can turn off Getting to Know You at any time. This will stop the data collection for this feature and will delete associated data stored on your device, such as your local user dictionary and your input history. Because Cortana uses this data to help understand your input, turning off Getting to Know You will also disable speech recognition in Cortana. At <https://www.bing.com/account/personalization>, you can also sign in with your personal Microsoft account and clear data sent to Microsoft, such as your contacts and calendar data, as well as search and browsing history if your device also had Cortana enabled.

## Sync Settings

---

When you sign into 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 into one or more devices with a Microsoft account, when you sign into 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 Windows Store
- Language preferences
- Ease of Access preferences
- Personalization settings such as your account picture, background, and mouse settings
- Settings for Windows 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 Sync Settings in the Accounts section of Windows Settings. Some apps have their own, separate sync controls. If you sign into 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.

## Telemetry & Error Reporting

---

As you use Windows, we collect diagnostic and usage data that helps us identify and troubleshoot problems, improve our products and services, and provide you with personalized experiences. 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 three levels of diagnostic and usage data: **Full**, **Enhanced** and **Basic**. You can select which level of diagnostic and usage data to provide, but some diagnostic data is vital to the operation of Windows and cannot be turned off.

During Windows setup, opting to "Send full error and diagnostic reporting to Microsoft" sets your **Diagnostic and usage data** setting to **Full**. If you don't choose to "Send full error and diagnostic reporting to Microsoft," **Diagnostic and usage data** collection will be set to **Enhanced**. You can adjust your Diagnostic and usage data collection level at any time in **Settings**. We recommend that you select **Full** for the best Windows experience and the most effective troubleshooting.

**Basic** data is data that is vital to the operation of Windows. This data helps keep Windows and apps secure, up-to-date, and running properly by letting Microsoft know the capabilities of your device, what is installed, and whether Windows is operating correctly. This option also includes basic error reporting back to Microsoft. Basic data includes:

- Configuration data, including the manufacturer of your device, model, number of processors, display size and resolution, date, region and language settings, and other data about the capabilities of the device.
- The software (including drivers and firmware supplied by device manufacturers), installed on the device.
- Performance and reliability data, such as which programs are launched on a device, how long they run, how quickly they respond to input, how many problems are experienced with an app or device, and how quickly information is sent or received over a network connection.
- Network and connection data, such as the device's IP address, number of network connections in use, and data about the networks you connect to, such as mobile networks, Bluetooth, and identifiers (BSSID and SSID), connection requirements and speed of Wi-Fi networks you connect to.
- Other hardware devices connected to the device.

**Enhanced** data includes all **Basic** data plus data about how you use Windows, including Microsoft and third party software (apps, drivers, etc.) that runs on Windows. This data includes how you use certain features or apps and for how long, which apps and features you use most often, how often you use Windows Help and Support, and which services you use to sign into apps. This option also lets us collect diagnostic data related to system or app crashes. If you select this option, we'll also be able to provide you with an enhanced and more personalized Windows experience.

**Full** data includes all **Basic** and **Enhanced** data, plus additional diagnostic data including the memory state of your device when a system or app crash occurs (which may unintentionally include parts of a document you were using when a problem occurred). It also turns on advanced diagnostic features that can collect additional data from your device, which helps us further troubleshoot and fix problems. When devices experience problems that are difficult to diagnose or replicate with Microsoft's internal testing, Microsoft will randomly select a small number of devices, from those at the Full level and exhibiting the problem, from which to gather all of the data needed to diagnose and fix the problem (including user content that may have triggered the issue). If an error report contains personal data, we won't use that information to identify, contact, or target advertising to you.

Windows error reports help Microsoft and Microsoft partners diagnose problems in the software you use and provide

solutions. We provide limited portions of error report information to partners (such as OEMs) 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.

## 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 Windows Store are automatically updated through the Store, as described in the [Store](#) section above.

## Web Browsers: Microsoft Edge and Internet Explorer

---

Microsoft Edge is Microsoft's default web browser for Windows. Internet Explorer, Microsoft's legacy browser, 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, 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.

New features in Microsoft Edge allow you to capture and save content on your device, such as:

- **Web Note:** which allows you to create ink and text annotations on the web pages you visit, and clip, save or share them;
- **Active Reading:** which allows you to create and manage reading lists including websites or documents; and
- **Hub:** which allows you to easily manage your reading lists, favorites, downloads, and history all in one area.

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 and reading lists. 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 Sync Settings in the Accounts section of Windows Settings (see [Sync Settings](#)). 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:

- **AutoSearch and Search Suggestions** in Internet Explorer automatically sends the information you type into the browser address bar to your default search provider (such as Bing) and offer search recommendations as you type each character. In Microsoft Edge, this feature automatically sends this information to Bing even if you have selected another default search provider.
- **Page Prediction** sends your browsing history to Microsoft and uses aggregated browsing history data to predict which pages you are likely to browse to next and proactively loads those pages in the background for a faster browsing experience.
- **Suggested Sites** recommends web contents that you might be interested in based on your search and browsing history.

Browsing data collected in connection with these features is used in the aggregate and you can turn off any of these features at any time. These features will not collect browsing history while you have InPrivate Browsing enabled.

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. Separately, if you enable Cortana to use your browsing history in Cortana Permissions, Microsoft will collect your Microsoft Edge search queries and full browsing history, associated with a user ID. Cortana and related Microsoft products will use this data to learn about you and provide you with timely and intelligent answers and proactive personalized suggestions, or to complete web tasks for you. You can disable Cortana's access to your browsing history at any time in Cortana Permissions. To learn more about how Cortana uses data and how you can control that, go to the [Cortana](#) section of this privacy statement.

## Wi-Fi Sense

---

Wi-Fi Sense allows you to automatically connect to Wi-Fi networks around you to help you save cellular data and give you more connection options. If you turn it on, you will automatically connect to open Wi-Fi networks. Please note that not all open networks are secure - be careful using an open network to do something online that requires sensitive or personal data, such as making a banking transaction or a purchase.

## Windows Apps

---

A number of Microsoft apps are included with Windows and others are available in the Windows 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. Please see the [Bing](#) section of this privacy statement to learn more about these Bing-powered experiences. 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's 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). See [Sync Settings](#) above for more information.

**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.

Your photos, videos, as well as screenshots, saved in your camera roll automatically upload to OneDrive. You can manage your photos and/or videos in OneDrive, and you can disable the automatic upload in Settings.

When you take photos embedded with your location, the Photos app can group your photos by time and location. To group your photos, the Photos app sends location data in your photos to Microsoft to determine the names of locations, such as "Seattle, Washington". When you are using the Photo app while signed into your Microsoft account, your photos and videos from OneDrive will be automatically sorted into albums in the Photo app, and will also appear on the Photo app's live tile. Your photos and/or videos will only be shared with others if you choose to do so.

**People app.** The People app lets you see and interact with all your contacts in one place. When you add your Microsoft account to a Windows device, 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. 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's 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 from storage, you must 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.

**Microsoft Wallet.** You can use Microsoft Wallet to hold information such as coupons, loyalty cards, tickets, and other digital content. Where available, you can also add payment cards to the Microsoft Wallet to make payments at participating stores using NFC (near-field communication).

You can set up your wallet for payment by logging into Microsoft Wallet with your personal Microsoft account and adding payment cards associated with your Microsoft account. When you add a payment card to Microsoft Wallet, we provide data to your bank and payment card network, including your name, card number, billing address, email address, device data (including the device name, type, and identifier), and your location at the time you add your payment card to your wallet. This data is sent to your bank and payment card network to determine the eligibility of your payment card, enable transactions, detect fraud.

When you make an NFC payment, Microsoft Wallet will provide the merchant with an encrypted version of your payment card (a “token”). The merchant will present this token, along with transaction details, to your bank to complete the transaction and request payment for your transaction.

## 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 picture or image of your face 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 OneDrive as well as on your device. If you choose to use Windows Search to search the web, or get search suggestions with Windows Search or Cortana, 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.

## Xbox

---

Xbox consoles are hardware devices that you can use to access and play games, movies, music, and other forms of digital entertainment. Xbox Live (including Games for Windows Live) is Microsoft's online gaming and entertainment service and social network. It provides ways for you to connect with your friends on Xbox Live and other gaming and social networks. Xbox services can be accessed from a variety of devices, including Xbox consoles, PCs (including via xbox.com and the Xbox app), and mobile devices.

We collect data about your use of Xbox services, such as:

- When you sign in and sign out, the games you play, your game and score statistics, and the purchases you make and content you obtain.
- Performance data about the Xbox services, your device and your network connection, including any hardware or software errors that occur.
- If you use the Xbox console with Kinect, data about how you use Kinect. See below for more information about Kinect data collection.

All such data is stored with the Xbox console's unique identifier and associated with your personal data. When your Xbox is connected to the Internet, we identify which console and which version of the Xbox operating system you are currently using.

With your consent, we will collect information about videos you purchase or view through third-party apps on your Xbox console. 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.

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 into the services on the console, usage data will be stored on the storage device and sent to Microsoft the next time you sign into the services.

**Xbox Live data viewable by other users.** Your gamertag (Xbox live nickname), game and score statistics, achievements, presence (whether you're signed into Xbox Live), and other data about your activity on Xbox Live can be seen by other users on Xbox Live or 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 types of data, you can adjust your privacy settings on the console or at [xbox.com](https://xbox.com) to limit or block the sharing with other users.

**Xbox Live data shared with game or app publishers.** When you use an Xbox Live-enabled game or app, the publisher or service provider for that game or app has access to data about your usage of Xbox Live and that game or app, and may disclose or display (such as on leaderboards) such data. This data includes, for example, your game scores, data about your game play sessions (for example, types of vehicles used in the game), your presence on Xbox Live, the time you spend playing the game or app, rankings, statistics, gamer profiles, avatars, and other content that you may create or submit within the game or app.

**Linking your Xbox Live account to non-Microsoft accounts.** Some of the games or apps found on Xbox Live are delivered by partner companies, which may require that you create a non-Microsoft account and sign-in credentials to use that game or app. If you choose to link your Microsoft account with your account with a partner company, Microsoft will share limited account information with that company. Such account information can include name, address, email and date of birth but will not include any credit card or other payment information. For games that enable in-game communications, the game publisher will also have access to the content of in-game communications when you are signed into your account with the publisher.

**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 into 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](https://skype.com).

To learn more about Kinect, please visit the [Kinect FAQ](#).

**Communications monitoring.** Xbox Live includes communications features such as text-based messaging and online voice chat between players during gameplay. In order to help provide a safe gaming environment and enforce the [Microsoft Code of Conduct](#), we will collect, review, and monitor a sample of these communications, including Xbox Live game chats and party chat communications in live-hosted multiplayer gameplay sessions offered through the services.

**Voice data for service improvement.** We collect, and use for service improvement, voice search requests or samples of voice commands occurring while using Kinect. These data are 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. Microsoft can review game clips for violations of the [Microsoft Code of Conduct](#), even if your game clip sharing setting is set to Block.

**Xbox Live Rewards.** Xbox Live Rewards, available at [rewards.xbox.com](https://rewards.xbox.com), is a program you can join to receive Xbox credits for being active on the services. You must agree to receive promotional communications from the Rewards program as a condition of joining. You sign into Rewards using your Microsoft account, and the program collects personal data including first name, last name, gamertag, and demographic information. The program is hosted and operated by HelloWorld, a Microsoft vendor. The data collected is stored by the vendor on behalf of Microsoft. You can review and edit the personal data you provided to the Rewards

program by contacting [privacy@helloworld.com](mailto:privacy@helloworld.com).

**Children and online safety.** If you have children who use Xbox services, you can set up child accounts for them. Children 17 and younger cannot create an account on Xbox Live without parental consent. Adults in the family can change consent choices and online safety settings for child accounts on [xbox.com](https://xbox.com).

## Enterprise Products

---

Enterprise Products are those Microsoft products and related offerings that are offered or designed primarily for use by organizations and developers. They include subscription cloud services, such as Office 365, Microsoft Azure, Microsoft Dynamics CRM Online, Microsoft Intune, and Yammer, for which an organization (our "customer") contracts with Microsoft for the services ("Online Services"). They also include server and developer products customers run on their own premises, such as Windows Server, SQL Server, Visual Studio, and System Center ("On-Prem Products").

Some Enterprise Products have their own, separate privacy statements. ***In the event of a conflict between a Microsoft privacy statement and the terms of any agreement(s) between a customer and Microsoft, the terms of those agreement(s) will control.***

When a customer purchases or subscribes to Enterprise Products, or obtains support for such products, Microsoft collects data to provide the best experiences with our products, operate our business, 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 organization, to support that engagement.
- When a customer interacts with a Microsoft support professional, we collect support 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 a customer receives communications for Microsoft, we use data to personalize the content of the communication.

Our customers, in turn, may administer the Enterprise Products to end users. If you use a work or school account (i.e. an email address provided by your organization, such as your employer or school) to sign into Enterprise Products, the owner of the domain associated with your email address may: (i) control and administer your account and (ii) access and process your data, including the contents of your communications and files. Microsoft is not responsible for the privacy or security policies or practices of our customers, which may differ from those of Microsoft. If your organization is administering your use of the Enterprise Products, please direct your privacy inquiries to your administrator.

**Online Services.** The Online Services collect Customer Data and Administrator Data. "Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, you or your end users through use of the Online Service. Customer Data is used only to provide the customer the Online Services including purposes compatible with providing those services. For example, we may use Customer Data to provide a personalized experience, improve service reliability, combat spam or other malware, or improve features and functionality of the Online Services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. For more information about the features and functionality that enable you to control Customer Data, please review documentation specific to the Online Service. To learn more about Microsoft's handling of Customer Data, including information about how we handle data access requests and security, please see [Microsoft Online Services Terms](#).

"Administrator Data" is data provided to Microsoft during sign-up, purchase, or administration of the Online Services. 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. We use Administrator Data to provide the Online Services, complete transactions, service the account, and detect and prevent fraud. Administrator Data may also include 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 Online Services; we may contact those individuals with communications that may 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 Online Services, including information about new features, security or other technical issues. We may also contact you regarding third-party inquiries we receive regarding use of the Online Services, as described in your agreement. You will not be able to unsubscribe from these non-promotional communications. Subject to your contact preferences, we may also contact you regarding information and offers about other products and services, or share your contact information with Microsoft's partners. You may manage your contact preferences or update your information in your account profile.

When you use social features of the Online Services, other users in your network may see some of your activity. To learn more about the social features and other functionality, please review documentation specific to the Online Service.

The Online Services enable you to purchase, subscribe to or use other Microsoft products. Please be sure to read the product-specific details for each product you use to understand how each products' privacy practices may differ.

**On-Prem Products.** On-Prem Products collect data to operate effectively and provide you the best experiences. The data we collect depends on the features you use, but it is generally limited to usage data. Customers have choices about the data they provide. For example:

- During installation or when you upgrade an On-Prem Product, we may collect use and performance data to learn whether you experience any difficulties.
- When you use On-Prem Products, we may collect device data to learn about your operating environment to improve security features.
- When you experience a crash, 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 On-Prem Products to provide and improve our products, to deliver customer support, to activate the product, to communicate with you, and to operate our business.