Microsoft

Microsoft Privacy Statement

Last Updated: April 2018 What's new?

Your privacy is important to us. This privacy statement explains what personal data Microsoft collects from you, through our interactions with you and through our products, and how we use that data.

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

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

Personal Data That 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, administer your organisation's licensing account, submit a search query to Bing, register for a Microsoft event, speak a voice command to Cortana, upload a document to OneDrive, purchase an MSDN subscription, sign up for Office 365 or contact us for support. We get some of it by 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. We protect data obtained from third parties according to the practices described in this statement, plus any additional restrictions imposed by the source of the data. These third-party sources vary over time, but have included:

- Data brokers from which we purchase demographic data to supplement the data we collect.
- Social networks when you grant permission to a Microsoft product to access your data on one or more networks.
- Service providers that help us determine a location based on your IP address in order to customise certain products to your location.

- Partners with which we offer co-branded services or engage in joint marketing activities, and
- Publicly-available sources such as open government databases or other data in the public domain.

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 context of your interactions with Microsoft, the choices you make, including your privacy settings, and the products and features you use. The data we collect 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.

Device and Usage data. We collect data about your device and 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 search queries or commands to Bing, Cortana and our chat bots. This also includes the settings you select and the software configurations you use most.
- *Device, connectivity and configuration 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 (sometimes called "crash dumps") 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.
- *Troubleshooting and Help Data*. When you engage Microsoft for troubleshooting and help, we collect data about you and your hardware, software and other details

related to the incident. Such data includes contact or authentication data, the content of your chats and other communications with Microsoft, 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 favourites. We collect data about your interests and favourites, such as the teams you follow in a sports app, the programming languages you prefer, the stocks you track in a finance app or the favourite cities you add to a weather app. In addition to those you explicitly provide, your interests and favourites 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, for example Outlook.com, or to communicate or interact with other people or organisations, for example Visual Studio Team Services.

Location data. For products with location-enhanced features, we collect data about your location, which can be either precise or imprecise. Precise location data can be Global Navigation Satellite System (GNSS) data (e.g. GPS), 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 postcode level.

Content. We collect content of your files and communications when necessary to provide you with the products you use. For example, if you transmit a file using Skype to another Skype user, we need to collect the content of that file to display it to you and the other user as you direct. If you receive an email using Outlook.com, we need to collect the content of that email to deliver it to your inbox, display it to you, enable you to reply to it and store it for you until you choose to delete it. Other data we collect to provide communication services to you include 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.

Video. If you enter Microsoft Store locations or other facilities, or attend a Microsoft event, your image may be captured by our security cameras.

If you use Spend, at your direction, we may also collect payment card information, receipt data or financial transaction data, to provide the service.

If you use Enterprise Online Services, Microsoft collects the data defined below in the Enterprise and Developer Products section.

We also collect information you provide to us and 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.

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 personalising) the products we offer, (2) to send communications, including promotional communications, and (3) to show advertising, whether in our own products supported by advertising like MSN and Bing, or in products offered by third parties.

In carrying out these purposes, we combine data that we collect to give you a more seamless, consistent and personalised experience. For example, Cortana can use the favorite sports teams you add to the Microsoft Sports app to provide information relevant to your interests, Microsoft Store can use information about the apps and services you use to make personalised 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, developing new features, conducting 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 personalised features and recommendations that enhance your productivity and enjoyment, and automatically tailor your product experiences based on the data we have about 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 – such as 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. For example, we use error reports to improve security features, search queries and clicks in Bing to improve the relevancy of the search results, usage data to determine what new features to prioritise, and 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 licences, 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, some of our communications and file syncing products, such as Outlook or OneDrive, systematically scan content in an automated manner to identify suspected spam, viruses, abusive actions or URLs that have been flagged as fraud, phishing or malware links; and we 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 communicate with you and personalise our communications with you. For example, we may contact you by phone or email or other means to inform you when a subscription is ending, discuss your licensing account, let you know when security updates are available, remind you about items left in your online shopping basket, update you or enquire 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, post and telephone. For information about managing your contact data, email subscriptions and promotional communications, please visit the Access and Controls section of this privacy statement.

Advertising. Microsoft does not use what you say in email, chat, video calls or voicemail, or your documents, photos or other personal files to target ads to you.

We use data we collect through our interactions with you, through some of our products and on third-party web properties, to show advertising. For example:

- Microsoft may use your data to select and deliver some of the ads you see on Microsoft web properties, such as Microsoft.com, MSN and Bing.
- When the advertising ID is enabled in Windows 10 as part of your privacy settings, Microsoft apps can access and use the advertising ID (much the same way that websites can access and use a unique identifier stored in a cookie) to select and deliver ads in such apps.
- We may share data we collect with third parties, such as Oath, AppNexus or Facebook (see below), so that they can select and deliver some of the ads you see in our products, their products or other sites and apps serviced by these partners.
- 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 Oath, AppNexus or Facebook, to permit them to provide services on our behalf or to partner with us in selecting and serving ads for our advertising partners.

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

The ads that you see may also be selected based on other information learned about you over time using demographic data, location data, search queries, interests and favourites, usage data from our products and sites, as well as the sites and apps of our advertisers and partners. We refer to these ads as "interest-based advertising" in this statement. For example, if you view gaming content on xbox.com, you may see offers for games on MSN. To provide interest-based advertising, we combine cookies placed on your device using information that we collect (such as IP address) when your browser interacts with our websites. If you opt out of receiving interest-based advertising, data associated with these cookies will not be used.

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 programmes:
  - 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)
- **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 that we have collected on their sites or ads.
- **Data Collected by Other Advertising Companies**. Advertisers sometimes include their own web beacons (or those of their other advertising partners) within their advertisements that we display, enabling them to set and read their own cookie. Additionally, Microsoft partners with third-party ad companies to help provide some of our advertising services, and we also allow other third-party ad companies to display advertisements on our sites. These third parties may place cookies on your computer and collect data about your online activities across websites or online services. These companies currently include, but are not limited to: A9, AppNexus, Criteo, Facebook, MediaMath, nugg.adAG, Oath, Rocket Fuel, Yahoo!. You may find more information about each company’s practices, including the choices that it offers, by clicking on the company’s name 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 authorised. 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 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 belonging to 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 that we disclose in response to requests from law enforcement and other government agencies, please see our Law Enforcement Transparency Report, available at www.microsoft.com/en-gb/about/corporate-responsibility/lerr/.

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, edit or delete 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 privacy dashboard.** You can see and control activity data across multiple Microsoft services on the Microsoft privacy dashboard at: account.microsoft.com/privacy. From here, you can view, and clear browsing, search and location data associated with your Microsoft account. You can also manage data in your Cortana Notebook and Microsoft Health services.
- **Volume Licensing Service Center (VLSC)**. From here, you can gain easy access to all your licensing information in one location.
- **Microsoft account**. If you wish to access, edit or remove the profile information and payment information in your Microsoft account, change your password, add security information or close your account, you can do so by visiting account.microsoft.com. From here, you can also access controls for other Microsoft products.
- **Skype**. If you wish to access, edit or remove profile information and payment information in your Skype account or change your password, you can sign into your account at 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 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 Centre.
- If you have a Microsoft Developer Network public profile, you can access and edit it at connect.microsoft.com/profile.aspx.

If you cannot access certain personal data collected by Microsoft via the links above or directly via the Microsoft products that 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, postal 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 those messages. You can also make choices about the receipt of promotional email, telephone calls and post by signing in with your personal Microsoft account, and viewing your communication permissions where you can update contact information, manage Microsoft-wide contact preferences, opt out of email subscriptions and choose whether to share your contact information with Microsoft partners. If you do not have a personal Microsoft account, you can manage your Microsoft email contact preferences by using this web form. These choices do not apply to mandatory service communications that are part

of certain Microsoft 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 that you are using. The opt-out cookie has an expiry 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.

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

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 that 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 that you visit indicating that 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 that 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 to 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 additional identifiers, such as the advertising ID in Windows, for similar purposes, and many of our websites and applications also contain web beacons or other similar technologies, as described below.

Our Use of Cookies and Similar Technologies

Microsoft uses cookies and similar technologies for several purposes, depending on the 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 postcode 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. We also save preferences, such as language, browser and multimedia player settings, so those do not have to be reset each time 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. You can also save your sign-in information so you do not have to sign in each time you return to the site.
- **Security**. We use cookies to detect fraud and abuse of our websites and services.
- **Storing Information You Provide to a Website**. When you provide information, or add products to a shopping basket when shopping on Microsoft websites, we store the data in a cookie to remember the products and information you have added.
- **Social Media**. Some of our websites include social media cookies, including those that enable users who are logged in to the social media service to share content via that service.
- **Feedback**. Microsoft uses cookies to enable you to provide feedback on a website.
- **Interest-Based Advertising**. Microsoft uses cookies to collect data about your online activity and identify your interests so that we can provide advertising that is most relevant to you. You can opt out of receiving interest-based advertising from Microsoft as described in the Access and Control section of this privacy statement.
- **Showing Advertising**. Microsoft uses cookies to record how many visitors have clicked on an advertisement and to record which advertisements you have seen so you don't see the same one repeatedly.
- **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. This includes cookies from Microsoft and from third-party analytics providers.
- **Performance**. Microsoft uses cookies for load balancing to ensure that websites remain up and running.

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

- **MUID, MC1 and MSFPC** - Identifies unique web browsers visiting Microsoft sites. These cookies are used for advertising, site analytics and other operational purposes.
- **ANON** - Contains the ANID, a unique identifier derived from your Microsoft account, which is used for advertising, personalisation and operational purposes. It is also used to preserve your choice to opt out of interest-based advertising from Microsoft if you have chosen to associate the opt-out with your Microsoft account.
- **CC** - Contains a country code as determined from your IP address.
- **PPAuth, MSPAuth, MSNRPSAuth, KievRPSAuth** - Helps to authenticate you when you sign in with your Microsoft account.
- **NAP** - Contains an encrypted version of your country, postcode, 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.
- **MR** - Used to collect information for analytics purposes.
- **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:

- Adjust: www.adjust.com/opt-out
- AppsFlyer: www.appsflyer.com/optout
- Clicktale: www.clicktale.net/disable.html
- Flurry Analytics: https://aim.yahoo.com/aim/us/en/optout/
- Google Analytics: tools.google.com/dlpage/gaoptout (requires you to install a browser add-on)
- Kissmetrics: kissmetrics.com/user-privacy
- Mixpanel: mixpanel.com/optout
- Nielsen: www.nielsen-online.com/corp.jsp?section=leg_prs&nav=1#Optoutchoices
- Visible Measures: www.visiblemeasures.com/viewer-settings-opt-out
- WebTrends: 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 behaviour. These technologies include Local Shared Objects (or “Flash cookies”) and Silverlight App Storage.

Local Shared Objects or “Flash cookies”. Websites that use Adobe Flash technologies can use Local Shared Objects or “Flash cookies” to store data on your computer. To manage or block Flash cookies, go to www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html.

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

Notice to End Users

Many Microsoft products are intended for use by organisations and are administered to you by your organisation. Your use of Microsoft products may be subject to your organisation's policies, if any. If your organisation is administering your use of the Microsoft products, please direct your privacy enquiries to your administrator. When you use social features of such products, other users in your network may see some of your activity. To learn more about the social features and other functionality, please review documentation or help content specific to the Microsoft product. Microsoft is not responsible for the privacy or security practices of our customers, which may differ from those set forth in this privacy statement.

If you use an email address provided by an organisation you are affiliated with, such as an employer or school, to access Microsoft online services, the owner of the domain (e.g. your employer) associated with your email address may: (i) control and administer your Microsoft online services account and (ii) access and process your data, including the contents of your communications and files.

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 personalisation, provides seamless and consistent experiences across products and devices, permits you to access and use cloud data storage, allows you to make payments using payment instruments stored in your Microsoft account and enables other enhanced features and settings. When you sign 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. 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. If you chose to make payments to third-party merchants using your Microsoft account, Microsoft will pass to the third party information stored in your Microsoft account necessary to process your payment and fulfill your order (such as name, credit card number, billing and delivery addresses, and relevant contact information). The third party can use or share the data it receives when you sign in or make a purchase according to its own practices and policies. **You should carefully review the privacy statement for each product you sign into and each merchant you purchase from 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.**

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 organisation, 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 organisation's policies, if any. Microsoft is not responsible for the privacy or security practices of these organisations, which may differ from those of

Microsoft. If your organisation is administering your use of Microsoft products, please direct your privacy inquiries to your administrator. See also: Notice to End Users.

Other Important Privacy Information

Below, you will find additional privacy information that you may find important. You can also find more information on Microsoft's commitment to protecting your privacy at privacy.microsoft.com.

European Privacy Rights

Microsoft adheres to applicable data protection laws in the European Economic Area, which if applicable includes the following rights:

- If the processing of personal data is based on your consent, you have a right to withdraw consent at any time for future processing;
- You have a right to request from us, a "data controller" as defined in the law, access to and rectification of your personal data;
- You have a right to object to the processing of your personal data; and
- You have a right to lodge a complaint with a data protection authority.

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

When we process personal data about you, we do so with your consent and/or as necessary to provide the products you use, operate our business, meet our contractual and legal obligations, protect the security of our systems and our customers, or fulfill other legitimate interests of Microsoft as described in the "How We Use Personal Data" and "Reasons We Share Personal Data" sections above. When we transfer personal data from the European Economic Area, we do so based on a variety of legal mechanisms, as described in "Where We Store and Process Personal Data" below.

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, and in any other country where Microsoft or its affiliates,

subsidiaries or service providers operate facilities. Microsoft maintains major data centres in Australia, Austria, Brazil, Canada, Chile, Finland, France, Germany, Hong Kong SAR, India, Ireland, Japan, Korea, Luxembourg, Malaysia, the Netherlands, Singapore, South Africa, the United Kingdom and the United States. Typically, the primary storage location is in the customer's region or in the United States, often with a backup to a data centre in another region. The storage location(s) are chosen in order to operate efficiently, to improve performance and to create redundancies in order to protect the data in the event of an outage or other problem. We take steps to ensure that the data we collect under this privacy statement is processed according to the provisions of this statement and the requirements of applicable law wherever the data is located.

We transfer personal data from the European Economic Area and Switzerland to other countries, some of which have not been determined by the European Commission to have an adequate level of data protection. When we do, we use a variety of legal mechanisms, including contracts, to help ensure your rights and protections travel with your data. To learn more about the European Commission's decisions on the adequacy of the protection of personal data in the countries where Microsoft processes personal data, please visit: ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

Microsoft Corporation complies with the EU-US Privacy Shield Framework and Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use and retention of personal information transferred from the European Union and Switzerland to the United States. Microsoft Corporation has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If third-party agents process personal data on our behalf in a manner inconsistent with the principles of either Privacy Shield framework, we remain liable unless we prove we are not responsible for the event giving rise to the damage. The controlled US subsidiaries of Microsoft Corporation, as identified in our self-certification submission and listed here, also adhere to the Privacy Shield Principles.

If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield programme, and to view our certification, please visit www.privacyshield.gov.

If you have a question or complaint related to Microsoft's participation in the EU-US or Swiss-US Privacy Shield, we encourage you to contact us via our web form. For any complaints related to the Privacy Shield frameworks that cannot be resolved with Microsoft directly, we have chosen to cooperate with the relevant Data Protection Authority, or a panel established by the European DPAs for resolving disputes. Please contact us to be directed to the relevant DPA contacts. As further explained in the Privacy Shield Principles, binding arbitration is available to address residual complaints not resolved by other means. Microsoft is subject to

the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

Our Retention of Personal Data

Microsoft retains personal data for as long as necessary to provide the products and fulfill the transactions you have requested, or for other essential purposes such as complying with our legal obligations, resolving disputes and enforcing our agreements. Because these needs can vary for different data types in the context of different products, actual retention periods can vary significantly. The criteria used to determine the retention periods include:

- *How long is the personal data needed to provide the products and operate our business?* This includes such things as maintaining and improving the performance of those products, keeping our systems secure and maintaining appropriate business and financial records. This is the general rule that establishes the baseline for most data retention periods.
- *Do customers provide, create or maintain the data with the expectation we will retain it until they affirmatively remove it?* Examples include a document you store in OneDrive, or an email message you keep in your Outlook.com inbox. In such cases, we maintain the data until you actively delete it, such as by moving an email from your Outlook.com inbox to the Deleted Items folder, and then emptying that folder (when your Deleted Items folder is emptied, those emptied items remain in our system for up to 30 days before final deletion).
- *Is there an automated control, such as in the Microsoft privacy dashboard, that enables the customer to access and delete the personal data at any time?* If there is not, a shortened data retention time will generally be adopted.
- *Is the personal data of a sensitive type?* If so, a shortened retention time would generally be appropriate.
- *Has Microsoft adopted and announced a specific retention period for a certain data type?* For example, for Bing search queries, we de-identify stored queries by removing the entirety of the IP address after 6 months, and cookie IDs and other cross-session identifiers after 18 months.
- *Has the user provided consent for a longer retention period?* If so, we will retain data in accordance with your consent.
- *Is Microsoft subject to a legal, contractual or similar obligation to retain the data?* Examples can include mandatory data retention laws in the applicable jurisdiction, government orders to preserve data relevant to an investigation or data that must be retained for the purposes of litigation.

Preview or Free of Charge Releases

Microsoft offers preview, insider, beta or other free-of-charge products and features ("previews") to enable you to evaluate them while providing 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 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, complaint or a question for the Chief Privacy Officer/Data Protection 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. You can contact the data protection officer of Microsoft Ireland Operations Limited at the following address: Microsoft Ireland Operations, Ltd., Attn: Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland.

Skype Communications S.à.r.l. 23-29 Rives de Clausen L-2165 Luxembourg, Luxembourg is a data controller for Skype. To contact us in relation to Skype software or products, please submit a support request to the Skype customer support team.

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

Enterprise and Developer Products

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

- Cloud services referred to as Online Services in the Microsoft Online Services Terms (OST), such as Office 365, Microsoft Azure, Microsoft Dynamics365, Microsoft Intune and Yammer, for which an organisation (our customer) contracts with Microsoft for the services ("Enterprise Online Services").
- Server and developer products, such as Windows Server, SQL Server, Visual Studio and System Centre ("Enterprise and Developer Software").
- Appliances and hardware used for storage infrastructure, such as StorSimple ("Enterprise Appliances"); and
- Developer services such as Bot Framework, Cortana Skills Kit and Botlet Store.
- Professional services referred to in the OST that are available with Enterprise Online Services, such as onboarding services, data migration services, data science services or services to supplement existing features in the Enterprise Online Services.

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

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

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

General. When a customer tries, purchases, uses or subscribes to Enterprise and Developer Products, or obtains support or professional services with for such products, Microsoft collects data to provide the service, including uses compatible with providing the service, 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 customer's organisation, to support that engagement.
- When a customer interacts with a Microsoft support professional, we collect Device and Usage data or error reports to diagnose and resolve problems.
- When a customer pays for products, we collect contact and payment data to process the payment.
- When a customer receives communications from Microsoft, we use data to personalise the content of the communication.
- When a customer engages with Microsoft for professional services, we collect the name and contact data of the customer's designated point of contact and use information provided by the customer to perform the services that the customer has requested.

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

Enterprise Online Services

To provide the Enterprise Online Services, Microsoft collects Customer Data, Administrator Data, Payment Data and Support Data.

We use Customer Data, Personal Data, and Support Data as described in the OST and the Microsoft Trust Center.

Administrator Data is the information provided to Microsoft during sign-up, purchase or administration of Enterprise Online Services. We use Administrator Data to provide the Enterprise Online Services, complete transactions, service the account and detect and prevent fraud. Administrator Data includes the name, address, phone number and email address you provide, as well as aggregated usage data related to your account, such as the controls you select. Administrator Data 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 Enterprise 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 Enterprise 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 Enterprise 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.

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

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

Bing Search Services, as defined in the OST, use data such as search queries as described in the Bing section of this Privacy Statement.

Enterprise and Developer Software and Enterprise Appliances

Enterprise and Developer Software and Enterprise Appliances collect data to operate effectively and provide you the best experiences. The data we collect depends on the features you use, as well as your configuration and settings, but it is generally limited to Device and Usage data. Customers have choices about the data they provide. For example:

- During installation or when you upgrade an Enterprise and Developer Software, we may collect Device and Usage data to learn whether you experience any difficulties.
- When you use Enterprise Software or Enterprise Appliances, we may collect Device and Usage data to learn about your operating environment to improve security features.
- When you experience a crash using Enterprise Software or Enterprise Appliances, you may choose to send Microsoft an error report to help us diagnose the problem and deliver customer support.

Microsoft uses the data we collect from Enterprise and Developer Software and Enterprise Appliances to provide and improve our products, to deliver customer support, to activate the product, to communicate with you and to operate our business.

Microsoft SQL Server is a relational database management platform and includes products that can be installed separately (such as SQL Server Management Studio). For detailed information about what data we collect, how we use it, and how to manage your privacy options, please see go.microsoft.com/fwlink/?linkid=868444. If you work in an organisation, your administrator can set certain telemetry settings via Group Policy.

Productivity and Communications Products

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

Office

Office is a collection of productivity 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 services, such as Bing, and third-party connected services. For detailed information about how to manage your privacy options, please see go.microsoft.com/fwlink/?LinkId=624445. If you work in

an organisation, 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 customised 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 customised 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 customised 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 apps, 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 Centre > Trust Centre 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 that 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 authorisation data indicating you have the right to download the relevant content. Frequently, the information that you receive will include 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 that you want to translate isn't in the bilingual dictionary included with your app 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 app 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 organisation's use of Office 365.

When you use OneDrive, we collect data about your usage of the service, as well as the content that 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 personalised experiences, such as enabling you to sync content across devices and roam customised 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 in to your account and then select the specific content to manage the permission levels. Revoking permissions for a link effectively deactivates the link. No one will be able to use the link to access the content unless you decide to share the link again.

Files managed with OneDrive for Business are stored separately from files stored with your personal OneDrive. OneDrive for Business collects and transmits personal data for authentication, such as your email address and password, which will be transmitted to Microsoft and/or to the provider of your Office 365 service.

Outlook

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

Outlook.com. Outlook.com is 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, personalised 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 organisation (such as your employer or school), the owner of the organisational domain can implement policies and controls (for example, requiring multi-factor authentication or the ability to remotely wipe data from your device) that can affect your use of Outlook.

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

Skype

Skype lets you send and receive voice, video and instant message communications. This section applies to the consumer version of Skype; if you are using Skype for Business, see the Enterprise and Developer Products section of this privacy statement. 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 Skype public 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 until you tell us to stop. 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 such as traffic data and details of purchases made by other members of the group who have consented to such access. If you add information such as 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.

Skype marketing affiliate programme. So that more people can learn about Skype, we encourage other companies and organisations to sign up as marketing affiliates to refer people to Skype. When the people they refer do things such as buying 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 that we can know which marketing affiliate made a successful referral and earned a payment. Microsoft does not 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 another company. To tell you who is calling, for example, or to give you the first few words of the new chat, Skype has to tell the notification service so that they can provide the notification to you. The company providing the notification service on your device will use this information in accordance with their own terms and privacy policy. Microsoft is not responsible for the data collected by the company providing the notification service. If you don't want to use the notification services for incoming Skype calls and messages, turn it off in the settings found in the Skype application or your device.

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 account.microsoft.com/privacy. 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.

Search and Artificial Intelligence

Search and Artificial Intelligence products connect you with information and intelligently sense, process and act on information – learning and adapting over time.

Bing

Bing services include search and mapping services, as well as the Bing Toolbar and Bing Desktop apps. Bing services 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 that 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. Additionally, if you use Bing voice-enabled services, 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 for 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, while using Bing Search, go to Bing settings. Search Suggestions cannot be turned off in Cortana. On Windows, you can always hide Cortana and the search box so as not to use the feature.

Bing Experience Improvement Programme for Bing Desktop and Bing Toolbar. If you are using Bing Desktop or Bing Toolbar and choose to participate in the Bing Experience Improvement Programme, we also collect additional data about how you use these specific Bing apps, such as the addresses of the websites that you visit, to help improve search ranking and relevance. To help protect your privacy, we do not use the data collected via the Bing Experience Improvement Programme to identify or contact you, or target advertising to you. You can turn off

the Bing Experience Improvement Programme at any time in the Bing Desktop or Bing Toolbar settings. Finally, we delete the information collected via the Bing Experience Improvement Programme 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.

Personalisation 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 personalisation features to customise your interests, favourites and settings, and to connect your account with third-party services. Visit the Bing Settings page to manage your personalisation settings or the Microsoft privacy dashboard.

Managing Search History. Bing's Search History service provides an easy way to revisit the search terms that you've entered and results that you've clicked when using Bing search in your browser. You may clear your search history on the Microsoft privacy dashboard at https://account.microsoft.com/privacy. 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 that your browser sends to every website that you visit – such as your IP address, browser type and language, and the URL of the site that 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 that you entered (which could include names, addresses or other identifying information), the destination website will be able to determine the search term that 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, including voice queries, 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 National Insurance 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. Depending on the capabilities of your device and the version of Cortana you are using (e.g. Windows, Xbox, iOS, etc.), Cortana can provide a range of features, some of them personalised. Cortana works best when you sign in and let her use data from your device, your personal Microsoft account, your AAD account, other Microsoft services and third-party services you choose to connect. On Windows devices, if you choose not to sign in to Cortana, you can still chat with Cortana and use Cortana to help you search the web, or for your email, people and documents stored on your device or in Microsoft services, like OneDrive. See the subsection on Windows Search for more information. But if you don't sign in, your experiences will be more limited and will not be personalised. On iOS, Android devices and other Cortana enabled devices, Cortana works only when you sign-in.

Signed out. When you are not signed in on a Windows device, 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 Services**. 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 personalised.
- **Queries and search history**. Your Bing search queries and the Search Suggestion feature – even if Cortana does the searching for you – are treated like any other Bing search queries and are used as described in the Bing section.
- **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 in 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 personalised experiences and relevant suggestions; and you give Cortana permission to collect or access the following additional types of data, some of which depend on the capabilities of the version of Cortana you are using (e.g. Windows, Android, iOS, etc.) and the app or device you are using into which Cortana is integrated (e.g. Skype):

- **Microsoft account**. Cortana can access the demographic data (such as your age, postcode 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 personalised suggestions. For example, Cortana uses data collected by the Sports app, so it can automatically display information about the teams you follow. It also learns your favourite places from Microsoft's Maps app, your favourite songs and artists from the music you play in Groove Music, and what you view and purchase in Microsoft 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 customise your interests, preferences and favourites 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). Location data Cortana collects is used to provide you personalised experiences across our products, such as making your Bing search results more relevant, and it may also be used in de-identified form to improve the Windows Location Services. See more details in the Location Services subsection.

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

- **Contacts, text messages and email**. Cortana accesses your contacts and messages to do a variety of things such as: making calls when Cortana is connected to Skype, allowing you to add events to your calendar, apprising you of important messages or important contacts and keeping you up to date on events or other things that are important to you, like package or commitment tracking. Cortana also uses your contacts and 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 browsing history, Microsoft will collect your Microsoft Edge search queries and full browsing history, associated

with a user ID. Cortana will use this data to learn about you and provide you with timely and intelligent answers and personalised suggestions, or to complete web tasks for you. Cortana won't collect information about sites you visit in InPrivate tabs.

Other Connected Services and managing Skills. You can also give Cortana access to data collected by other Microsoft and third-party services, or share your Cortana information with those services, by giving your permission to enable or connect those services with Cortana. When you enable a Connected Service or third-party Skill, Cortana shares your request with those services or third parties to enable your command; Cortana may also share additional information that you give permission to share (e.g. your location). Information you share with a third party when using a Connected Service or third-party Skill is governed by the third party's privacy statement and terms of use. Cortana uses your queries and responses from interactions with Connected Services or third-party Skills to improve its speech recognition and user-intent understanding and to provide you personalised suggestions and features. Below are examples of Connected Services and Skills. New Connected Services and Skills are added regularly.

- **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 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 and relationships. Choosing to sign into LinkedIn within Cortana allows Microsoft to access your LinkedIn data so that Cortana can give you more personalised information and recommendations. Note, Cortana enables LinkedIn to access the name, email address, job title and company name of people are you are meeting with, in order for Cortana to retrieve relevant information about those contacts.
- **Other Connected services and Skills**. Cortana allows you to connect to third-party services to enable her to do more and provide additional personalised experiences based upon data from the third-party service. Not all Skills require your authentication. With your permission, ***Cortana can also send information about you along with your request to a third-party.*** For instance, Cortana will send your request, along with your current location and destination, to Uber when you ask Cortana to request a ride. You can manage Cortana's Connected Services and Skills in the Cortana Notebook.

When you provide Cortana with permission to access your information from a device or service, this information may be used to seamlessly personalise your Cortana experience on any device or service on which you have enabled Cortana. Remember that you can always sign out of Cortana. When you sign out on Windows, Cortana will still be there to help, but your experiences will not be personalised. 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.

Microsoft Translator

Microsoft Translator is a statistical machine translation system designed to automatically translate text and speech between numerous supported languages. Translator may be incorporated into other Microsoft products and services, such as Office, SharePoint and Bing. Third parties may also incorporate Translator into their own services and offerings. For information about the privacy practices of third parties' services and offerings, consult their privacy statements.

Microsoft Translator collects and uses the text, image and speech data that you submit, as well as information about how you are accessing the Translator service, such as operating system version, browser type and language. We use your data to provide the Translator service, which includes improving and personalising your experiences. Microsoft has implemented business and technical measures designed to help de-identify the data that Translator retains. For example, we randomly sample text to improve Translator and delete strings of numbers and other personally identifiable information we detect in the sample.

If you subscribe to the Microsoft Translator API with a monthly volume of 250 million characters or more, you may request to have logging turned off for the text you submit to Microsoft Translator by submitting a request using the process detailed at https://www.microsoft.com/en-us/translator/notrace.aspx.

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 personalised 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 personalisation, prediction synchronisation and backup. Our prediction technology learns from the way you use language to build a personalised language model. This model is an optimised 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 personalisation 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 personalised 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 organisation (such as your employer or school), your organisation may use centralised management tools provided by Microsoft or others to control device settings, device policies, software updates, data collection by us or the organisation, or other aspects of your device. For more information about data collection and privacy in Windows, go to 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 licence to the software. This data may be sent again if there is a need to re-activate or validate your licence. On phones running Windows, device and network identifiers, as well as device location at the time of the first power up of the device, are also sent to Microsoft for the purpose of warranty registration, stock replenishment and fraud prevention.

Activity History

Activity history in Windows 10 helps keep track of the things you do on your device. Activity history keeps track of the apps and services you use, the files you open and the websites you browse – and when you do these things. Your activity history is collected and stored locally on your device, and if you've signed into your device with a Microsoft account and given your permission, Windows sends your

activity history to Microsoft. Once your activity history has been collected, Microsoft uses that data to enable cross-device experiences, to provide you with personalised experiences and relevant suggestions, and to help improve Microsoft products.

Activity history is also created and sent to Microsoft when you use Microsoft apps, such as Microsoft Edge, and Office apps like Word, Excel and PowerPoint, on mobile devices such as iOS and Android phones and tablets. If you are signed in with your Microsoft account, you can continue activities on your Windows device that you started in Microsoft apps on your Android or iOS device.

Advertising ID

Windows generates a unique advertising ID for each user on a device. When the advertising ID is enabled, apps (both Microsoft apps and third-party apps) can access and use the advertising ID in much the same way that websites can access and use a unique identifier stored in a cookie. Thus, your advertising ID can be used by app developers and advertising networks to provide more relevant advertising and other personalised experiences across their apps and on the web. Microsoft collects the advertising ID for the uses described here only when you choose to enable the advertising ID as part of your privacy setting. You can turn off access to this identifier at any time by turning off the advertising ID in your privacy settings (in Start > Settings > Privacy). 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.

Diagnostics

There are two levels of diagnostic data: Basic and Full. Microsoft uses diagnostic data to keep Windows secure and up-to-date, troubleshoot problems and make product improvements. Regardless of your selection your device will be just as secure and operate normally. This data is transmitted to Microsoft and stored with one or more unique identifiers that can help us recognise an individual user on an individual device and understand the device's service issues and usage patterns.

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

- Device, connectivity and configuration data:
  - Data about the device such as the processor type, OEM manufacturer, type of battery and capacity, number and type of cameras, firmware and memory attributes.
  - Network capabilities and connection data such as the device's IP address, mobile network (including IMEI and mobile operator) and whether the device is connected to a free or paid network.

    - Data about the operating system and its configuration such as the OS version and build number, region and language settings, diagnostics level and whether the device is part of the Windows Insider programme.
    - Data about connected peripherals such as model, manufacturer, drivers and compatibility data.
    - Data about the applications installed on the device such as application name, version and publisher.
- Whether a device is ready for an update and whether there are factors that may impede the ability to receive updates, such as low battery, limited disk space or connectivity through a paid network.
- Whether updates complete successfully or fail.
- Data about the reliability of the diagnostics collection system itself.
- Basic error reporting, which is health data about the operating system and applications running on your device. For example, basic error reporting tells us if an application, such as Microsoft Paint or a third-party game, hangs or crashes.

Full data includes everything collected with Basic data, plus additional information about device health, device usage and enhanced error reporting that helps Microsoft to fix and improve products and services for all users. We collect the following additional information at the Full level:

- Additional data about the device, connectivity and configuration, beyond that collected at Basic.
- Status and logging information about the health of operating system and other system components (in addition to data about the update and diagnostics systems collected at Basic).
- App usage, such as which programs are launched on a device, how long they run and how quickly they respond to input.
- Browser usage, including browsing history and search terms, in Microsoft browsers, Microsoft Edge or Internet Explorer.
- Enhanced error reporting, including the memory state of the device when a system or app crash occurs (which may unintentionally contain user content, such as parts of a file you were using when the problem occurred). Crash data is never used for Tailored experiences as described below.

Some of the data described above may not be collected from your device even if your diagnostic data setting is set to Full. Microsoft minimises the volume of data it collects from all devices by collecting some of the data at the Full level from only a subset of devices (sample). By running the Diagnostic Data Viewer tool, you can see an icon which indicates whether your device is part of a sample and also which specific data is collected from your device. Instructions for how to download the Diagnostic Data Viewer tool can be found at **Start** > **Settings** > **Privacy** > **Diagnostics & feedback**.

Specific data items collected in Windows diagnostics are subject to change to give Microsoft flexibility to collect the data needed for the purposes described. For

example, to ensure Microsoft can troubleshoot the latest performance issue impacting users' computing experience or update a Windows 10 device that is new to the market, Microsoft may need to collect data items that were not collected previously. For a current list of data types collected at both levels of diagnostics, see go.microsoft.com/fwlink/?linkid=870052 or see go.microsoft.com/fwlink/?linkid=844962 for the current list of data collected at Basic.

We provide limited portions of error report information to partners (such as OEMs) to help them troubleshoot products and services that 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.

Inking and Typing. In addition to the data collected at **Basic** or **Full**, you can separately choose to help Microsoft improve inking and typing recognition by sending Inking and Typing diagnostic data. If you choose to do so, Microsoft will collect samples of the content you type or write to improve features such as handwriting recognition, autocompletion, next word prediction and spelling correction in the many languages used by Windows customers. When Microsoft collects Inking and Typing diagnostic data, it is divided into small samples and processed to remove unique identifiers, sequencing information and other data (such as email addresses and numeric values) which could be used to reconstruct the original content or associate the input to you.

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

Tailored experiences include suggestions on how to customise and optimise Windows; and recommendations for and offers of Microsoft and third-party products and service, features, apps and hardware for your Windows experiences. For example, to help you get the most out of your device, we may tell you about features you may not know about or that are new. If you are having a problem with your Windows device, you may be offered a solution. You may be offered a chance to customise your lock screen with pictures or to be shown more pictures of the kind you like, or fewer of the ones you don't. If you stream films in your browser, you may be recommended an app from the Microsoft Store that streams more efficiently. Or, if you are running out of space on your hard drive, Windows may recommend you try OneDrive or purchase hardware to gain more space.

Location Services, Motion Sensing, & Recording

Windows location service. Microsoft operates a location service that helps determine the precise geographic location of a specific Windows device. Depending on the capabilities of the device, location is determined using satellite Global Positioning System (GPS) data, detecting nearby mobile phone masts and/or WiFi access points and comparing that information against a database that Microsoft maintains of mobile phone masts and WiFi access points whose location is known, or deriving your location from your IP address. When the location service is active on a Windows device, or you have given permission for Microsoft apps to access location information on non-Windows devices, data about mobile-phone towers and WiFi 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, postcode or region.

Find My Phone. The Find My Phone feature allows you to find the location of your Windows phone from 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 the 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 centre.

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 that a fitness app can estimate how many calories you burn. This data and history is stored on your device and can be accessed by apps that you give permission to access and use that data.

Recording. Some Windows devices have a recording feature that allows you to capture audio and video clips of your activity on the device, including your communications with others. If you choose to record a session, the recording will be saved locally on your device. In some cases, you may have the option to transmit the recording to a Microsoft product or service that broadcasts the recording publicly. **IMPORTANT: You should understand your legal responsibilities before recording and/or transmitting any communication. This includes whether you need to get consent from all parties to the communication in advance.** Microsoft is not responsible for how you use recording features or your recordings.

Security and Safety Features

Device encryption. Device encryption helps protect the data stored on your device by encrypting it using BitLocker Drive Encryption technology. When device encryption is on, Windows automatically encrypts the drive that 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 does not 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.

Windows Defender SmartScreen. Windows Defender SmartScreen helps protect you when using our services by checking downloaded files and web content for malicious software, potentially unsafe web content and other threats to you or your device. When checking a file, data about that file is sent to Microsoft, including the file name, a hash of the file's contents, the download location and the file's digital certificates. If Windows Defender SmartScreen identifies the file as unknown or potentially unsafe, you will see a warning prior to opening the file. When checking web content, data about the content and your device is sent to Microsoft, including the full web address of the content. If Windows Defender SmartScreen detects that content is potentially unsafe, you will see a warning in place of the content. Windows Defender SmartScreen can be turned on or off in Settings.

Windows Defender Antivirus. Windows Defender Antivirus looks for malware and other unwanted software on your device. Windows Defender Antivirus is automatically turned on to help protect your device if no other antimalware software is actively protecting your device. If Windows Defender Antivirus is turned on, it will monitor the security status of your device. When Windows Defender Antivirus is turned on, or is running because Limited Periodic Scanning is enabled, it will automatically send reports to Microsoft that contain data about suspected malware and other unwanted software, 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 Antivirus not to send reports and suspected malware to Microsoft.

Speech, Inking and Typing

Windows provides both a device based speech recognition feature (available through the Windows Speech Recognition Desktop app), and a cloud-based speech recognition service that was introduced alongside Cortana in those markets and regions where Cortana is available. Go here https://support.microsoft.com/instantanswers/557b5e0e-0eb0-44db-87d6-5e5db6f9c5b0/cortana-s-regions-and-languages to learn what languages and regions speech currently supports. When you use cloud-based speech recognition, Microsoft collects and uses your voice input to provide you with speech recognition services in Cortana and other supported applications.

Additionally, your typed and handwritten words are collected to provide you a personalised 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 that 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.

As part of the cloud-based speech recognition service, we also collect information from the user dictionary created on your device. Both the voice data and the user dictionary are collected and used in the aggregate to help improve our ability to correctly recognise all users' speech.

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 favourite places, apps you use and information about your music preferences. This additional data enables us to better recognise people, events, places and music when you dictate commands, messages or documents.

You can turn cloud speech recognition off 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.

Sync Settings

When you sign in to Windows with a Microsoft account, Windows syncs some of your settings and data with Microsoft servers to make it easier to have personalised experiences across multiple devices. After you've signed in to one or more devices with a Microsoft account, when you sign in to another with the same Microsoft account for the first time, Windows will download and apply the settings and data that you choose to sync from your other devices. Settings that 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 Microsoft Store
- Language preferences
- Ease of Access preferences
- Personalization settings such as your account picture, background, and mouse settings
- Settings for Microsoft Store apps
- Spell checker dictionaries, input method editor (IME) dictionaries, and personal dictionaries
- Internet Explorer browser history, favourites and websites that you have open
- Saved app, website, mobile hotspot and WiFi 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 in to Windows with a work account and you choose to connect that account to your personal Microsoft account, Windows will ask which settings you want to sync before connecting your Microsoft account.

Update Services

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

Windows Update automatically downloads Windows software updates to your device. You can configure Windows Update to automatically install these updates as they become available (recommended) or have Windows notify you when a restart is required to finish installing updates. Apps available through Microsoft Store are automatically updated through Microsoft Store, as described in the Microsoft 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 that 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, favourites, downloads and history, all in one area.

Some Microsoft browser information that is 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 favourites; and in Microsoft Edge, it includes your favourites, reading lists and autofill form entries, such as your name, address and phone number. 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:

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

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

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

WiFi Connecting to suggested open hotspots

If you turn it on Connect to suggested open hotspots in WiFi settings, you will automatically connect to suggested open WiFi networks. Please note that not all 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 Microsoft Store. Some of those apps include:

Maps app. The Maps app provides location-based services and uses Bing services to process your searches within the Maps app. When Maps App has access to your location, and you have enabled location-based services in Windows, when you use the "@" key to initiate a search in supported text boxes in Windows apps, Bing services collects the text you type after the "@" key to provide location-based suggestions. 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 favourite places and recent map searches in the Maps app. Your favourite places and search history will be included as search suggestions. If you're signed in with your Microsoft account, your favourite 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 that you take with your device. Other descriptive data, such as the 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 and screenshots that are saved in your camera roll are automatically uploaded 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 in to 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 an account to the People app, your contacts from your account will be automatically added to the People app. You can add other accounts to the People app, including your social networks (such as Facebook and Twitter) and email accounts. When you add an account, we tell you what data the People app can import or sync with the particular service and let you choose what you want to add. Other apps that you install may also sync data to the People app,

including providing additional details to existing contacts. When you view a contact in the People app, information about your recent interactions with the contact (such as emails and calendar events, including from apps that the People app syncs data from) will be retrieved and displayed to you. You can remove an account from the People app at any time.

Mail and Calendar app. The Mail and Calendar app allows you to connect all your email, calendars and files in one place, including those from third-party email and file storage providers. The app provides location-based services, such as weather information in your calendar, but you can disable the app's use of your location. When you add an account to the Mail and Calendar app your email, calendar items, files, contacts and other settings from your account will automatically sync to your device and to Microsoft'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 organisation (such as a company email address), the owner of the organisational 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 App for Windows Phone. 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 and 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 Media Player

Windows Media Player allows you to play CDs, DVDs and other digital content (such as WMA and MP3 files), rip CDs and manage your media library. To enrich your experience when you play content in your library, Windows Media player displays related media information, such as album title, song titles, album art, artist and composer. To augment your media information, Windows Media player will send a request to Microsoft which contains standard computer information, an identifier for the media content and the media information already contained in your Windows Media Player library (including information you may have edited or entered yourself) so that Microsoft can recognise the track and then return additional information that is available.

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

Windows Hello

Windows Hello provides instant access to your devices via 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 does not leave your device. You can delete your biometric verification data from within Settings.

Windows Search

Windows Search lets you search your files and the web from one place. If you choose to use Windows Search to search "your stuff", it will provide results for items on your personal OneDrive, your OneDrive for Business if so enabled, other

cloud storage providers to the extent supported by those third-party providers, and on your device. If you choose to use Windows Search to search the web, or get search suggestions with Windows Search 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.

Entertainment and Related Services

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

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 does not 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 in to the services on the console, usage data will be stored on the storage device and sent to Microsoft the next time that you sign in to the services.

Xbox Live data viewable by other users. Your gamertag (Xbox live nickname), game and score statistics, achievements, presence (whether you're signed in to

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 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 in to 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 to enable gameplay. If you are playing online, we collect those numeric values to enable and improve gameplay and the gaming experience. Kinect also detects specific hand gestures intended to do simple system interactions (such as menu navigation, pan/zoom and scroll).
- For some fitness games, Xbox can use the Kinect sensor to estimate your exercise data, including estimates such as your heart rate during a certain activity or the number of calories burned during a workout.

- Kinect's microphones enable voice chat between players during gameplay. They also enable voice commands for control of the console, game or app or to enter search terms. See below for additional details on voice data collection.
- The Kinect sensor can also be used for audio and video communications through services such as Skype.

To learn more about Kinect, for Xbox 360, see Kinect and Xbox 360 privacy. For Xbox One, see Kinect and Xbox One Privacy.

Captioning. During Xbox real-time chat, players may activate a voice-to-text feature, which allows the user to view the audio in-game chat as text. If a user activates this feature, the other players will have no additional notice. Microsoft uses this data to provide captioning of chat for users who need it. We also use this data to improve our ability to provide the service and other, similar voice-based services.

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. This data is stored separately from your Xbox profile.

GameDVR. Any player in a multiplayer game session can use GameDVR to record their view of the gameplay taking place in that session. The recording can capture your in-game character and gamertag in the game clips created by other players in the gameplay session. Note that if a player uses GameDVR on a PC, audio chat may also be captured in a game clip. 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, is a programme you can join to receive Xbox credits for being active on the services. You must agree to receive promotional communications from the Rewards programme 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 programme by contacting privacy@helloworld.com.

Children and online safety. If you have children who use Xbox services, you can set up child accounts for them. Children aged 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.

Microsoft Store

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

- Apps and content for Windows devices such as phones, PCs and tablets,
- Games and other apps for Xbox consoles, and
- Products and apps for Office, SharePoint, Exchange, Access and Project (2013 versions or later).

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

Permission for Microsoft Store apps. Many apps you install from Microsoft Store are designed to take advantage of specific hardware and software features of your device. An app's use of certain hardware and software features may give the app or its related service access to your data. For example, a photo editing app might access your device's camera to let you take a new photo or access photos or videos stored on your device for editing, and a restaurant guide might use your location to provide nearby recommendations. Information about the features that an app uses is provided on the app's product description page in Microsoft Store. Many of the features that Microsoft Store apps use can be turned on or off through your device's privacy settings. In Windows, in many cases, you can choose which apps can use a particular feature. Go to **Start > Settings > Privacy**. Select the feature (for example, Calendar) and select which app permissions are on or off. The lists of apps in Windows privacy settings that can use hardware and software features will not include "Classic Windows" applications, and these applications are not affected by these settings.

App updates. Unless you have turned off automatic app updates in the relevant Microsoft Store settings, Microsoft Store will automatically check for, download and install app updates to ensure that you have the latest versions. Updated apps might use different Windows hardware and software features from the previous versions, which could give them access to different data on your device. You will be prompted for consent if an updated app accesses certain features, such as location. You can also review the hardware and software features an app uses by viewing its product description page in Microsoft Store.

Each app's use of your data collected through any of these features is subject to the app developer's privacy policies. If an app available through Microsoft Store

collects and uses any of your personal data, the app developer is required to provide a privacy policy, and a link to the privacy policy is available on the app's product description page in Microsoft Store.

Sideloaded apps and developer mode. Developer features such as the "developer mode" setting are intended for development use only. If you enable developer features, your device may become unreliable or unusable, and expose you to security risks. Downloading or otherwise acquiring apps from sources other than Microsoft Store, also known as "sideloading" apps, may make your device and personal data more vulnerable to attack or unexpected use by apps. Windows policies, notifications, permissions and other features intended to help protect your privacy when apps access your data may not function as described in this statement for sideloaded apps or when developer features are enabled.

MSN

MSN services include websites and a suite of apps, including MSN News, Weather, Sport and Money, and previous versions of the apps branded as Bing (together, “MSN Apps”). The MSN Apps are available on various platforms, including Windows, iOS and Android. MSN services are also included within other Microsoft services, including the Microsoft Edge browser.

When you install MSN Apps, we collect data that tells us if the app was installed properly, the installation date, the app version, and other data about your device such as the operating system and browser. This data is collected on a regular basis to help us determine the number of MSN App users and identify performance issues associated with different app versions, operating systems and browsers.

We also collect data about how you interact with MSN services, such as usage frequency and articles viewed, to provide you with relevant content. Some MSN services provide an enhanced experience when you sign in with your Microsoft account, including allowing you to customise your interests and favourites. You can manage personalisation through MSN and Bing settings, as well as through settings in other Microsoft services that include MSN services. We also use the data that 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.

Groove Music/Films & 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 sign into Cortana on your device, Microsoft will collect and use data related to the music you play via Groove Music to provide personalised 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 Films & TV to access content that has been protected with Microsoft Digital Rights Management (DRM), it may automatically request media usage rights from an online rights server and download and install DRM updates in order to let you play the content. See the DRM information in the Silverlight section of this privacy statement for more information.

Silverlight

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

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

Silverlight application storage. Silverlight-based apps 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 apps. You can turn off or configure app 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.

Microsoft Health Services

Microsoft Health services can help you understand and manage your health data. They include HealthVault, HealthVault Insights, Microsoft Band devices, other Microsoft Health applications and related products. 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 applications send data to Microsoft's servers and allow you to view, manage and control the data. The applications may enable notifications to the Band and other devices. HealthVault services let you gather, edit, add to and store health data online, along with 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 personalising 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.

Health Services

Microsoft Health services 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 Health services help 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 with the best service, we collect and automatically upload statistics about the performance and your use of the Microsoft Health services.
- **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 applications. 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 services. For example, 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 services. When you delete a specific activity, the event is deleted from the Microsoft Health services; however, other data and the basic sensor data captured by the devices remain in the Microsoft Health services. You can cancel your Microsoft Health services account at any time by contacting Customer Support here.

Cortana. The Microsoft Health services allow you to use Cortana. When you use Cortana, data you process in the Microsoft Health services, including health-related data and data processed from third-party services, is shared with Cortana. Cortana's capabilities allow you to perform queries and set reminders with your voice, if Cortana is enabled on your device. 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 applications, 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 third-party authentication services. 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, email address, postcode 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 US, HealthVault assigns each health record a unique HealthVault 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 that 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, including participating third-party services that you authorise. No service has access to your data through HealthVault unless an authorised 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 authorise for a record will get the full name associated with your HealthVault account, the nickname of the authorised 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 third-party 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 in Microsoft Health services 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 heath 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 summarising 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.

- Contact us
- Privacy & Cookies
- Terms of use

- Trademarks
- About our ads
- EU Compliance DoCs
- © Microsoft 2018