For up-to-date information on Microsoft’s data processing practices, please review the Microsoft Privacy Statement. Here you can also learn about the latest tools we provide to access and control your data and how to contact us if you have a privacy inquiry.

Windows Vista Privacy Statement

Highlight Statement Supplement

In this page

Windows Vista Privacy Notice Highlights

This notice provides highlights of the full Windows Vista Privacy Statement and explains at a high level some of the data collection and use practices of Windows Vista and all Windows Vista Service Packs. It focuses on features that communicate with the Internet and is not intended to be an exhaustive list. It does not apply to other online or offline Microsoft sites, products or services.

Find additional details about many of the data collection and use practices of Windows Server 2008.

Personal information

- Certain Windows Vista features may ask you for permission to collect or use your personal information. Additional information about these features and how they use your personal information is described in the full Windows Vista Privacy Statement.
- Some Windows Vista features allow you, with your permission, to share personal information over the Internet.
- If you choose to register your software, you will be asked to provide personal information.

- Additional details

Top of Page

Your choices

- You can choose whether to use or disable features of Windows Vista that transfer personal information over the Internet.
- A variety of controls are also available for features that transfer other types of information over the Internet.
- To make Windows Vista work better with the Internet, some features that do not collect personal information are turned on by default. You can choose to disable these features.
- Additional details

Top of Page

Uses of information

- We use the information collected to enable the features you are using or provide the services you request. We also use it to improve our products and services. If you choose to register, with your permission we use your personal information to request your feedback about the product or service that you are using; to provide critical updates and notifications regarding the software; or to provide you with advance notice of events or to tell you about new product releases.
- In order to help provide our services, we occasionally provide information to other companies that work on our behalf. These companies are required to keep this information confidential and are prohibited from using it for any other purpose.
- Additional details

Top of Page

Important information

- Windows Vista requires activation, to reduce software piracy and help ensure our customers receive the software quality they expect. Activation does not require any personal information.
- The full Windows Vista Privacy Statement contains links to supplementary information about specific Windows Vista features.
- An easily printable version of the full Windows Vista Privacy Statement with supplementary information can be downloaded here.
- For more information on how to help protect your personal computer, your personal information and your family online, visit our online safety resources.

Top of Page

How to contact us

For more information about our privacy practices, go to the full Windows Vista Privacy Statement. Or, you can write to us using our Web form.

Top of Page

For up-to-date information on Microsoft's data processing practices, please review the Microsoft Privacy Statement. Here you can also learn about the latest tools we provide to access and control your data and how to contact us if you have a privacy inquiry.

Windows Vista Privacy Statement

Highlight Statement Supplement

Windows Vista Privacy Statement

This statement covers Windows Vista and all Windows Vista Service Packs. For information about prior releases of Windows Vista, selected software that is part of the operating system, or related services, please refer to Privacy Statements for additional features and services on the right.

For information about specific features, please refer to Supplemental privacy information for Windows Vista features.

View the privacy notice highlights

Last Updated: November 2007

Microsoft is committed to protecting your privacy, while delivering software that brings you the performance, power and convenience you desire in your personal computing. Please read the Windows Vista Privacy Statement below and also any supplemental information listed to the right for additional details about many of the data collection and use practices of Windows Vista, and Microsoft services that you may use.

This disclosure focuses on features that communicate with the Internet and is not intended to be an exhaustive list. It does not apply to other Microsoft sites, services and products.

In this page

Privacy Statements for additional features and services

Windows Update

Windows Media Player

Windows Genuine Advantage

Microsoft Error Reporting Service

Windows Defender

Support Services

Windows Media Center

Internet Explorer

Digital Locker

Collection and use of your personal information

The personal information we collect from you will be used by Microsoft and its controlled subsidiaries and affiliates to provide the service(s) or carry out the transaction(s) you have requested or authorized, and may also be used to request additional information on feedback that you provide about the product or service that you are using; to provide important notifications regarding the software; to improve the product or service, for example bug and survey form inquiries; or to provide you with advance notice of events or to tell you about new product releases.

Except as described in this statement, personal information you provide will not be transferred to third parties without your consent. We occasionally hire other companies to provide limited services on our behalf, such as packaging, sending and delivering purchases and other mailings, answering customer questions about products or services, processing event registration, or performing statistical analysis of our services. We provide those companies the minimum personal information they need to deliver the service, and they are prohibited from using that information for any other purpose.

Microsoft may disclose personal information about you if required to do so by law or in the good faith belief that such action is necessary to: (a) comply with the law or legal process served on Microsoft; (b) protect and defend the rights of Microsoft (including enforcement of our agreements); or (c) act in urgent circumstances to protect the personal safety of Microsoft employees, users of Microsoft software or services, or members of the public.

Personal information collected by Microsoft software, sites and services may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries or agents maintain facilities, and by using Microsoft software, sites or services, you consent to any such transfer of information outside of your country. Microsoft abides by the safe harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Union.

Top of Page

Collection and use of information about your computer

Internet enabled features will send information about your computer ("standard computer information") to the websites you visit and web services you use. This information is generally not personally identifiable. Standard computer information typically includes information such as your IP address, operating system version, browser version, your hardware ID which indicates the device manufacturer, device name, and version and your regional and language settings. If a particular feature, software or service sends information to Microsoft, standard computer information will be sent as well. The privacy details for each Windows feature and Microsoft software or service listed here will disclose what additional information is collected and how it is used.

Top of Page

Your choice and control

You can choose whether to use or disable features of Windows Vista that transfer personal information over the Internet. You also can decide what personal information you wish to provide. A variety of controls are also available for features that transfer other types of information over the Internet. To make Windows Vista work better with the Internet, some features that do not collect personal information are turned on by default. You can choose to disable these features. For details about the information collection, uses, and choice provided by a specific feature or related product or service, please click on the link provided in the list.

Top of Page

Security of your information

Microsoft is committed to protecting the security of your information. We use a variety of security technologies and procedures to help protect your information from unauthorized access, use, or disclosure. For example, we store the information you provide on computer systems with limited access, which are located in controlled facilities. When we transmit highly confidential information (such as a credit card number or password) over the Internet, we protect it through the use of encryption, such as the Secure Socket Layer (SSL) protocol.

Top of Page

Changes to this privacy statement

We will occasionally update this privacy statement to reflect changes in our products and services and customer feedback. When we post changes to this Statement, we will revise the "last updated" date at the top of this statement. If there are material changes to this statement or in how Microsoft will use your personal information, we will notify you either by prominently posting a notice of such changes prior to implementing the change or by directly sending you a notification. We encourage you to periodically review this statement to be informed of how Microsoft is protecting your information.

Top of Page

For more information

Microsoft welcomes your comments regarding this privacy statement. If you have questions about this statement or believe that we have not adhered to it, please contact us by using our web form.

Microsoft Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052

Top of Page

For up-to-date information on Microsoft's data processing practices, please review the Microsoft Privacy Statement. Here you can also learn about the latest tools we provide to access and control your data and how to contact us if you have a privacy inquiry.

Windows Vista Privacy Statement

Highlight Statement Supplement

In this page

Windows Vista Privacy Supplement

Note that this page is a supplement to the Windows Vista Privacy Statement. In order to understand the data collection and use practices relevant for a particular feature, site, or service, you should read the Windows Vista Privacy Statement and any applicable supplement.

Last Updated: **December 2007**

Activation

What this feature does

Activation is aimed at reducing software counterfeiting, thereby helping to ensure that Microsoft customers receive the software quality that they expect. Once your software is activated, a specific product key becomes associated with the computer (the hardware) on which your software is installed. This association prevents the product key from being used to activate the same copy of the software on multiple computers as counterfeit software. Some changes to your computer components or the software may require you to reactivate the software.

Information collected, processed, or

- File Association Web Service
- Games Folder
- Handwriting Recognition (Available Only on Tablet PCs)
- Input Method Editor (IME)
- Installation Improvement Program
- Internet Printing
- Internet Protocol version 6 Network Address Translation Traversal
- Network Awareness
- Online Print Ordering Wizard
- Parental Controls
- Peer Name Resolution Service
- Plug and Play
- Plug and Play Extensions
- Program Compatibility Assistant
- Program Properties — Compatibility Tab
- Program Compatibility Wizard
- Properties

transmitted

During activation of this software, product key information is sent to Microsoft along with a hardware hash, which is a non-unique number generated from the computer's hardware configuration. The hardware hash does not represent any personal information or information about the software. The hardware hash cannot be used to determine the make or model of the computer and it cannot be backward calculated to determine any additional information about your computer. Along with standard computer information, some additional language settings are collected.

Use of information

Microsoft uses the information to confirm that you have a licensed copy of the software, and then it is aggregated for statistical analysis. Microsoft does not use the information to identify you or contact you.

Choice and control

Activation is mandatory and must be completed within a predefined grace period. If you choose not to activate the software, you cannot use it after the grace period expires. If the software is not correctly licensed, you will not be able to activate it.

Top of Page

Audit

What this feature does

Auditing allows an administrator to configure Windows to record operating system activity in a security log, which can be accessed using the Event Viewer and other programs. This log can help an administrator detect unauthorized access to the computer or resources on the computer, and to troubleshoot problems.

Information collected, processed, or transmitted

Administrators determine what information is collected, how

Registration

Rights Management Services (RMS) Client

Speech Recognizer

Trusted Platform Module (TPM) Services

Update Root Certificates

UPnP Technology

Windows Anytime Upgrade

Windows Calendar

Windows Collaboration Technologies

Windows Control Panel

Windows Help

Windows Mail

Windows Movie Maker

Windows Print Spooler

Windows Problem Reporting

Windows Terminal Services Client

Windows Time Service

long it is retained, and whether it is transmitted to other parties. The information can include personal information, such as user names or file names. For more information, contact your administrator.

Use of information

Administrators also determine how the audit information is used. Generally, the security log is used by auditors and administrators to track computer activity or to identify unauthorized access to the computer or resources on the computer.

Choice and control

Administrators determine whether this feature is enabled and how users are notified. The security log cannot be viewed by other users unless specifically permitted by an administrator.

Top of Page

BitLocker™ Drive Encryption

What this feature does

BitLocker Drive Encryption (BitLocker) is available on computers running Windows Vista™ Enterprise Edition and Windows Vista™ Ultimate Edition. Should your computer be lost or stolen, BitLocker protects your data by helping to prevent offline software attacks. Turning on BitLocker encrypts the hard drive where Windows is installed, including all information that is stored on that drive.

Information collected, processed, or transmitted

When BitLocker is turned on, cryptographic keys in memory continually encrypt and decrypt data as it is read from or written to the protected hard drive. During BitLocker setup, you can choose to print a recovery password or to save it to a USB flash drive or location on your network. In an enterprise environment, administrators can automatically save recovery information to Active Directory Domain Services. BitLocker associates one or more globally unique identifiers (GUIDs) with each protected hard drive to help manage each drive. These GUIDs are removed when BitLocker is disabled.

If your computer is equipped with the Trusted Platform Module (TPM) version 1.2 security hardware, BitLocker uses the TPM to provide hardware-enhanced data protection. For more information, see Trusted Platform Module (TPM) Services (below). On TPM-equipped computers, you can also set up a personal identification number (PIN) to add an extra layer of protection for your encrypted data. BitLocker will store this TPM-based PIN in a hashed and encrypted form on the hard drive.

Use of information

Cryptographic keys and GUIDs are stored in computer memory to support BitLocker operations. BitLocker recovery information allows you to access your protected data in case of hardware failures and other problems. This recovery information allows BitLocker to distinguish between authorized and unauthorized users. Information collected by BitLocker is not sent to Microsoft.

Choice and control

BitLocker is not turned on by default. An administrator can turn on or turn off BitLocker at any time by going to BitLocker Drive Encryption in Control Panel.

Top of Page

Crypto Application Programming Interface (API) Diagnostics

What this feature does

The Crypto API Diagnostics feature logs events associated with an application's use of certificates.

Information collected, processed, or transmitted

Information is collected about the certificates that you use, or that are used by the operating system and applications installed on your computer. Once this feature is enabled, the information is collected in an event log and can be viewed using Event Viewer.

Use of information

Administrators can use the information to identify and troubleshoot certificate trust issues. Administrators can also export the information to a file, for example, that can be sent to technical experts, such as Microsoft Premier Support, for analysis. No information is automatically sent to Microsoft.

Choice and control

The Crypto API Diagnostics feature is turned off by default, and it can be turned on or off only by an administrator. Unless you are experiencing a problem with certificates, you might not want to turn on this feature, which can decrease the performance of your computer. Administrators can configure Crypto API Diagnostics to log different parts of the certificate trust process, and they can determine the amount of information collected.

Top of Page

Customer Experience Improvement Program (CEIP)

What this feature does

If you choose to participate, basic information about your computer and how you use Windows Vista is collected in CEIP reports. Some limited information about the software you run on Windows Vista might also be collected to help improve how our products interact with that software. These reports are sent to Microsoft, where we use them to help improve the features our customers use most often and to create solutions to common problems.

Information collected, processed, or transmitted

CEIP reports generally include information about:

- **Configuration**, such as how many processors are in your computer, the number of network connections in use, screen resolutions for display devices, and which version of Windows is running. Reports can also include configuration information, such as the strength of the signal between your computer and a wireless or Bluetooth enabled device, and if some features such as high-speed USB connections are turned on.

- **Performance and reliability**, such as how quickly a program responds when you click a button, how many problems you experience with a program or a device, and how quickly information is sent or received over a network connection.
- **Program use**, such as the features that you use the most often, how often you use Windows Help and Support, and how many folders you typically create on your desktop.

CEIP reports also contain information about events (event log data) on your computer from up to seven days prior to the time you decide to participate in CEIP. Since most users decide to participate in CEIP within several days of setting up Windows, Microsoft uses this information to analyze and improve the Windows Vista setup experience.

This information is sent to Microsoft when you are connected to the Internet. CEIP reports do not contain personal information, such as your name, address, or phone number; however, some reports may unintentionally contain individual identifiers, such as a serial number for a device that is connected to your computer. Microsoft filters the information contained in CEIP reports to try to remove any individual identifiers that they might contain. To the extent that individual identifiers are received, Microsoft does not use them to identify you or contact you.

CEIP also generates a globally unique identifier (GUID) that is stored on your computer and sent with CEIP reports to uniquely identify your computer. The GUID is a randomly generated number that does not contain personal information.

Use of information

Microsoft uses CEIP information to improve our software. We use the GUID to distinguish how widespread the feedback we receive is and how to prioritize it. For example, the GUID allows Microsoft to distinguish between one customer experiencing a problem one hundred times and other customers experiencing the same problem once. Microsoft does not use the information collected by CEIP reports to identify you or contact you. Although the Internet Protocol (IP) address through which you access the Internet is sent to Microsoft with each CEIP report, Microsoft does not use it to identify you or contact you.

Choice and control

This feature is turned off by default. If you choose to participate, CEIP will collect the information described above for all users on your computer. Administrators can stop all users from participating in the Customer Experience Improvement Program by going to Problem Reports and Solutions in Control Panel. Click Control Panel, click System and Maintenance, click Problem Reports and Solutions and then, in the left pane, under See also, click Customer Experience Improvement Settings.

For more information, see these frequently asked questions about the Microsoft Customer Experience Program online at the Microsoft website.

Top of Page

Device Manager

What this feature does

Device Manager helps you install the latest drivers for your hardware devices. Using the Update Driver Software Wizard, you can update device drivers for hardware installed on your computer, modify hardware settings, and troubleshoot device and driver problems.

Information collected, processed, or transmitted

To determine which updates apply to your hardware, configuration information is collected from your computer and sent to Microsoft. Device Manager and the Update Driver Software Wizard work with Windows Update to collect this information. To learn more about the information collected by Windows Update and how it is used, see the Windows Update Privacy Statement online at the Microsoft website.

Use of information

The information collected is used to determine which updates apply to your computer hardware and to devices that you've installed. Microsoft does not use the information collected about your computer configuration to identify you or contact you.

Choice and control

Device Manager is enabled by default, and cannot be disabled. However, Device Manager will only send configuration information to Microsoft and download updated drivers when you open the Update Driver Software Wizard and choose to update your driver software. For more information about how to open Device Manager or how to use the Update Driver Software Wizard, see Windows Help and Support.

Top of Page

Dial-up Networking

What this feature does

Dial-up Networking allows you to access the Internet using a dial-up modem and a broadband technology, such as a cable modem and digital subscriber line (DSL). It also allows you to connect to private networks using a virtual private network (VPN) connection and Remote Access Service (RAS). RAS is a component that connects a client computer (typically your computer) to a host computer (also known as a remote access server) using industry standard protocols. VPN technologies allow users to connect to a private network, such as a corporate network, over the Internet.

Dial-up Networking includes dialer components such as RAS Client, Connection Manager, and RAS Phone, as well as command-line dialers like Rasdial.

Information collected, processed, or transmitted

The dialer component collects information from your computer, such as user names, passwords, domain names, and phone numbers. This information is sent to the system to which you are attempting to connect. The information is not sent to Microsoft. Security-related information, such as user names and passwords, is stored in an encrypted format on your computer.

The Connection Manager Administration Kit (CMAK) is a server component that allows administrators to build a user interface and collect information from users. Administrators determine which information is collected. For more information, contact your administrator.

Use of information

Dialer information is used to make connections to the Internet. For CMAK, the information is used to create connection profiles, which help administrators deploy and manage connections across a network.

Choice and control

For non-command line dialers, you can choose to save your password. This option is turned off by default, so you are prompted to provide your password to connect to the Internet or a network until the option is turned on and you choose to save your password. For command line dialers like Rasdial, there is no option to save your password.

Top of Page

Driver Protection

What this feature does

Driver Protection helps prevent the operating system from starting drivers that are known to cause stability problems.

These drivers are listed in a Driver Protection List database that is stored on your computer. Driver Protection checks this database while the operating system is running. These checks are performed to determine whether to start a driver. For more information, see the Driver Protection List article online at the Microsoft website.

Information collected, processed, or transmitted

Updated versions of required drivers are downloaded to your computer if you've enabled Windows Update. To learn more about the information collected by Windows Update and how it is used, see the Windows Update Privacy Statement. Administrators can also distribute updated versions of required drivers to computers on a network.

Use of information

Windows notifies you if a driver that is listed in the Driver Protection List starts. If you click the notification, Windows will ask if you want to report the problem to Microsoft so you can check for solutions or for more information. If you don't click the notification, Windows will automatically create a report and, depending on your problem reporting settings, ask you to send it later. To view or change your problem reporting settings, or to manually send reports at any time, use the options provided in Problem Reports and Solutions in Control Panel. To learn more about the information collected by Windows error reporting and how it is used, see the Privacy Statement for the Microsoft Error Reporting Service online at the Microsoft Online Crash Analysis (OCA) website.

If a driver is listed in the Driver Protection List during Windows setup, you will be notified before the operating system finishes installing. You can cancel setup and find an alternate driver solution before installing the operating system, or you can continue the setup process and install an alternate driver later. In this case, Windows might disable the driver in order to complete the installation. After the installation is complete and you log on, the operating system will notify you, as described above.

Choice and control

Driver Protection works with Windows Update and, during Windows setup, with Dynamic Update. To prevent Driver Protection from updating the Driver Protection List database on your computer, refrain from using Windows Update and Dynamic Update.

Top of Page

Dynamic Update

What this feature does

Dynamic Update enables Windows Vista to perform a one-time check with the Microsoft Update website to get the latest updates for your computer while your operating system is being installed. If updates are found, Dynamic Update automatically downloads and installs them so your computer is up to date the first time that you log on or use it.

Information collected, processed, or transmitted

The types of updates Dynamic Update can download to your computer include:

- **Installation updates:** Important updates for installation files to help ensure a successful installation.
- **In-box driver updates:** Important updates for the version of Windows that you are installing.

To install compatible drivers, Dynamic Update works with Windows Update to send information to Microsoft about your computer's hardware.

Use of information

Dynamic Update software reports information about your computer's hardware to find compatible drivers. For more information about how information collected by Dynamic Update is used, see the Windows Update Privacy Statement.

Choice and control

During Windows Vista setup, you can choose to use Dynamic Update.

Top of Page

Ease of Access Center

What this feature does

The Ease of Access Center enables you to turn on accessibility options and settings that can help you more easily interact with the computer.

Information collected, processed, or transmitted

The information collected is a list of impairments or difficulties that will be used to recommend settings on your computer to make it easier for you to use. You can provide this information by selecting the appropriate statements from a series.

These statements include:

- On TV, faces, or text are often hard to see clearly.
- I am colorblind.
- I am blind.
- I have an impairment that prevents me from using the keyboard.
- I am deaf.
- I have a speech impairment.

Use of information

This information is used to provide a set of configuration recommendations to you based on the statements that you chose. This information is saved in a non-human-readable format and stored locally on your computer. This information is not sent to Microsoft and is only available to you and to administrators on your computer, not to other users.

Choice and control

You can choose which statements you would like to select, and you can alter your choices at any time. You can also choose which recommendations you want to configure on your computer.

Top of Page

Event Viewer

What this feature does

Computer users, primarily administrators, can use Event Viewer to view and manage event logs. Event logs contain information about hardware and software problems and about security events on your computer. For example, application logs contain event information generated by all users and the programs that they use on the computer. By default, all users can view application log entries; however, administrators can choose to restrict access to Event Viewer logs.

Information collected, processed, or transmitted

You can access the event logs for your computer by opening Event Viewer. To learn how to open Event Viewer, see Windows Help and Support. To view event details, you can preview the event or view the event properties. A link to more information, called Event Log Online Help, is included both in the Event Properties dialog box and in the Event Preview pane. Unless you have previously consented to sending event information automatically, clicking the link will display a dialog box asking for your consent to send the information listed in the dialog box over the Internet. If you consent, the information is sent to a website to see if more information about the event is available, including solutions to problems that are recorded as an event. For Microsoft events, the event details will be transmitted to the Windows Server TechCenter on the Microsoft TechNet website. For events associated with third-party applications, the information will be transmitted to the site specified by the third-party publisher or manufacturer in their provider manifest. Administrators can use Group Policy to select or change the site to which event information is sent.

Use of information

Event information that is collected and sent to Microsoft when you click the Event Log Online Help link is used to locate and then provide you with additional information about the event. Microsoft does not use this information to contact you or identify you. If you send information about events to third-party publishers or manufacturers, use of the information will be subject to the third party's privacy practices.

Choice and control

When you click Event Log Online Help, you are asked to confirm that the information presented to you can be sent over the Internet. No event log information will be sent over the Internet unless you consent to send it. Administrators can use Group Policy to select or change the site to which event information is sent.

Top of Page

Fax

What this feature does

The fax feature allows you to create and save fax cover pages, and to send and receive faxes using your computer and an external or a built-in fax modem or a fax server.

Information collected, processed, or transmitted

Information collected includes any personal information entered on a fax cover page, as well as identifiers contained within industry standard fax protocols such as Transmitting Subscriber ID (TSID) and Call Subscriber ID (CSID). By default, Windows uses "Fax" as the value (name) for each identifier, but you can customize the TSID and CSID using the options provided in Fax Settings. The public viewing setting allows all users to see all received faxes in the system. This setting is on by default, but it can be altered by an administrator. If you send a fax, you are the only one who can see that sent fax; however, users with administrative privileges can manually locate and view all faxed documents on the computer.

Use of information

Information entered in the sender dialog box is presented on the cover page. Identifiers such as the TSID and CSID might contain arbitrary text and are typically used by the receiving fax machine or computer to identify the sender. No information is sent to Microsoft.

Choice and control

By default, fax access is determined by your user account privileges for the computer. Unless a fax administrator changes access settings, all users can send and receive faxes. All users can view the documents that they send and any fax that is received on the computer. Administrators can see all faxed documents, sent or received, and can configure fax settings, including who has permissions to view or manage faxes.

Top of Page

File Association Web Service

What this feature does

The file association web service helps users associate file types with specific applications. If you try to open a file type that does not have program associated with it, Windows will ask if you want to use the file association web service to find a program to open the file with. If you choose to use the service, it will send the file type extension to Microsoft. Applications that are typically associated with the file name extension are displayed.

Information collected, processed, or transmitted

If you choose to use the file association service, the file name extension is sent to Microsoft. Your computer display language is also sent to Microsoft.

Use of information

When you submit a file name extension, the service returns a list of the programs Microsoft is aware of, using your display language, that can open files of that extension. Unless you choose to download and install a program, the associations for the file type are not changed.

Choice and control

You choose whether to use the file association web service. No file association information is sent to Microsoft unless you decide to use the service. Administrators have several options to prevent users from using this service. For more information about administrative options, see the Using Windows Vista: Controlling Communication with the Internet article online at the Microsoft TechNet website.

Top of Page

Games Folder

What this feature does

The Games folder lists all of the games installed on your computer, giving you a single place to view and launch all of your games. The Games folder can also download and provide you with additional information (metadata) about those games such as box art, publisher information, descriptions, and reviews.

Information collected, processed, or transmitted

The Games folder optionally keeps track of the last time each game was played, to allow you to sort or filter the display of games. Information about when games were played is stored on your computer and is not sent to Microsoft. If you choose, the Games folder will retrieve metadata about the games you have installed from the Windows Metadata and Internet Services (WMIS) at Microsoft. To do this, information including the names of game files and shortcuts for the games will be sent to Microsoft.

Use of information

The information sent to Microsoft is used to retrieve metadata for the games that you've installed. Microsoft does not use the information to identify you or contact you. However, the information may be used to generate aggregate statistics.

Choice and control

You can turn the metadata collection or the tracking features of the Games folder on or off. When enabled, metadata will be retrieved each time that you open the Games folder, and the Games folder will track when games were last played. The first time that you open the Games folder, you can choose to retrieve and display game metadata and to track game playing times. You can disable these features by using the options that are provided in the Games folder. In an enterprise environment, administrators can use Group Policy to disable these features.

Top of Page

Handwriting Recognition (Available Only on Tablet PCs)

Personalization — Automatic Learning

What this feature does

Automatic learning is a handwriting recognition feature that is available on Tablet PCs. This feature collects data about the words that you use and how you write them. If you turn on automatic learning, the handwriting recognition software will attempt to recognize and improve its interpretation of your handwriting style and vocabulary.

Information collected, processed, or transmitted

Information collected by automatic learning is stored in the user profile for each user on the Tablet PC. This information is not sent to Microsoft. The data is stored in a proprietary format that cannot be read by using a text viewing program, such as Notepad or WordPad and is only available to you and to administrators on your computer, not to other users.

The information collected includes but is not limited to:

- Text from messages you compose and calendar entries you create by using e-mail programs such as Microsoft Office Outlook 2003 or Windows Mail, including any messages that you have already sent.
- Text that you type in the Internet Explorer address bar.
- Ink that you write in Tablet PC Input Panel.
- Recognized text from ink that you write in Input Panel.
- Alternate characters that you select to correct the recognized text.

Note

Automatic learning for both your handwriting style and your vocabulary might not be available for all languages in which handwriting personalization is offered. For more information on the type of data that is used for different languages, search Windows Help and Support for the topic "Handwriting personalization on a Tablet PC."

Use of information

The information collected is used to help improve handwriting recognition by creating a version of the recognition software that's personalized to your own style and vocabulary. The text samples are used to create an extended dictionary. The ink samples are used to help improve character recognition for each user on a Tablet PC.

Choice and control

You can turn automatic learning on or off at any time by using the Tablet PC settings in Control Panel. When you turn off automatic learning, any data that has been collected and stored by automatic learning is deleted.

Error Reporting for Handwriting Recognition

What this feature does

You can send reports to Microsoft about handwriting recognition errors that you encounter while using the Tablet PC Input Panel.

Information collected, processed, or transmitted

A short list of recently corrected handwriting samples is stored in memory. These handwriting samples are not written to your hard drive or sent to Microsoft without your explicit permission. No personal information is intentionally collected; however the samples you choose to send may include personal information. Microsoft does not use the information to identify you or contact you.

Use of information

You can select which recognition errors you would like to report. These reports are used to improve future versions of the Microsoft handwriting recognition software.

Choice and control

You can initiate a report using the Handwriting Recognition Error Reporting Tool; no reports are sent automatically. You can select each handwriting sample to be included in the report and review the report before sending it to Microsoft. In an enterprise environment, administrators can use Group Policy to disable Handwriting Recognition Error Reporting.

Top of Page

Input Method Editor (IME)

IME Learning

What this feature does

Microsoft Input Method Editor (IME) is used with East Asian languages to convert keyboard input to ideograms. The learning feature of IME for Simplified Chinese, Traditional Chinese, and Japanese may record words or word pairs to improve the selection of the ideograms displayed.

Information collected, processed, or transmitted

The IME learning feature records a word or word pair and their associated scores as a result of user operations. This information (excluding any digit/symbol character sequences) is stored in the user dictionary for each user on the computer. IME does not send the information to Microsoft.

Use of information

Learning data is used by IME on your system, and may also be referenced by Microsoft Office proofing tools. No information is sent to Microsoft.

Choice and control

The learning feature can be disabled by turning off the IME feature. The learning feature can also be enabled but configured not to write to the user dictionary.

IME Word Registration (available in Japanese IME only)

What this feature does

You can use word registration to report unsupported words (words that might not be converted correctly to ideograms from keyboard input).

Information collected, processed, or transmitted

Word registration reports can include the information you provide in the Add Word dialog box about the words being reported, and the software version number for IME. Personal information might unintentionally be collected, but Microsoft does not use the information to identify you or contact you. You will have the opportunity to review the data being sent with each report before you choose to send it.

Use of information

Word registration reports are sent to Microsoft using the Secure Socket Layer (SSL) protocol. Microsoft uses the information to help improve IME.

Choice and control

Each time a word registration report is generated, you are asked if you want to send this report to Microsoft. You may view the information contained in the report before choosing whether to send it. In an enterprise environment, administrators can use Group Policy to configure word registration reporting. Group Policy configuration options include the ability to completely turn off reporting, or to redirect reports to another server. For more information about using Group Policy to configure reporting, see Using Windows Vista: Controlling Communication with the Internet on the Microsoft TechNet website.

Top of Page

Installation Improvement Program

What this feature does

If you choose to participate in the Installation Improvement Program, the feature sends a single report to Microsoft. The report contains basic information about your computer and how you installed Windows Vista. We use this information to help improve the installation experience and to create solutions to common installation problems.

Information collected, processed, or transmitted

The report generally includes information about your installation and setup experience, such as the date of installation, the time it took for each installation phase to complete, whether the installation was an upgrade or a new installation of the product, version details, operating system language, media type, computer configuration, and success or failure status, along with any error codes.

The report is sent to Microsoft when you are connected to the Internet. This report does not contain contact information, such as your name, address, or phone number. A globally unique identifier (GUID) is generated and sent with the report. The GUID is a randomly generated number that uniquely identifies your computer; it does not contain personal information.

Use of information

Microsoft uses the report to improve our software installation experience. We use the GUID to correlate this data with data collected by the Customer Experience Improvement Program (CEIP), a program you can choose to participate in when you are using Windows Vista. This GUID enables us to distinguish how widespread the feedback we receive is and how to prioritize it. For example, the GUID allows Microsoft to distinguish between one customer experiencing a problem 100 times and 100 customers experiencing the same problem once. Microsoft will not use the information in the report to identify you or contact you.

For more information, see these frequently asked questions about the Microsoft Customer Experience Program online at the Microsoft website.

Choice and control

You can choose to participate in this program when you set up Windows Vista.

Top of Page

Internet Printing

What this feature does

Internet printing makes it possible for computers running Windows Vista to use printers located anywhere in the world by sending print jobs using Hypertext Transfer Protocol (HTTP).

Information collected, processed, or transmitted

When you print using this feature, you must first connect and authenticate yourself to an Internet print server. The information that you will need to submit to the print server will vary depending on the level of security that the print server supports (for example, you might be asked to provide a user name and password). Once you are connected, you are presented with a list of available printers. If your machine does not have a print driver for your selected printer, you may choose to download a driver from the print server. If you choose to use a print server hosted by Microsoft, Microsoft does not use the information that you provide to identify you or contact you.

Use of information

The information collected enables you to print using remote printers. If you send information to third-party print servers, use of the information will be subject to the third party's privacy practices.

Choice and control

You can enable or disable Internet printing by using the advanced options for Windows Features in Control Panel.

Top of Page

Internet Protocol version 6 Network Address Translation Traversal

What this feature does

The Internet Protocol version 6 (IPv6) Network Address Translation (NAT) Traversal service helps existing home Internet gateway devices transition from IPv4 to IPv6. IPv6 helps enable end-to-end connectivity that is often needed by peer-to-peer applications.

Information collected, processed, or transmitted

Each time you start up your computer, the NAT Traversal service will attempt to locate a public IPv6 Internet service by sending a query over the Internet. If you use a program (for example, Windows Meeting Space) that needs IPv6 connectivity, or if you configure your firewall to always enable IPv6 connectivity, then standard Domain Name Service (DNS) information will periodically be sent to the Microsoft IPv6 web service by default. No additional information is sent to Microsoft.

Use of information

This query sends standard DNS information to determine if your computer is connected to the Internet and if it can locate a public IPv6 service.

Choice and control

Using the netsh command line tool, you can change the query that the service sends over the Internet to use non-Microsoft servers instead, or you can turn off this feature.

Top of Page

Network Awareness

What this feature does

This feature collects Internet and intranet network connectivity information such as the Domain Name Service (DNS) suffix of your computer, forest name, and gateway address of networks that your computer connects to. The Network Awareness feature makes the connectivity information available through an application programming interface (API) to applications on your computer that might require the information to function properly.

Information collected, processed, or transmitted

No personal information is intentionally transferred or stored by this feature. Network connectivity profiles are stored in the registry. Network connectivity profiles can include the Network List Service, which provides a history of all networks visited and the date and time of the last connection.

Use of information

The information is not sent to Microsoft, but it is made available to applications on your computer that require network connectivity information.

Choice and control

The Network Location Awareness and Network List Services are on by default. An administrator can disable them using the options provided in the Services snap-in in Administrative Tools. Disabling them is not recommended because that will prevent some Windows features from functioning correctly.

Top of Page

Online Print Ordering Wizard

What this feature does

The Online Print Ordering Wizard enables you send digital pictures stored on your computer or network drive to an online photo printing service of your choice. Depending on the service, you can have your pictures printed and then delivered using postal mail, or you can pick up the prints at a local store.

Information collected, processed, or transmitted

If you decide to place an order with an online photo printing service, your selected digital photos are sent over the Internet to the service that you selected. The full path locations of the digital pictures that you select are also sent to the service in order to allow the service to display and upload the images. Digital picture files might contain data about the image that was stored with the file by the camera, such as the date and time that the picture was taken. The files might also contain personal information (such as captions) that may have been associated with the file through the use of digital picture management applications and Windows Explorer. For more information, see the "Properties" section later in this document.

Use of information

The information stored in the digital picture files by the camera may be used by the online photo printing service during the printing process, for example, to adjust the color or sharpness of the image before it is printed. Information stored by digital picture management applications may be used by the online photo printing service to print as captions on the front or back of the print copy. You should always consult the privacy statement of the online photo printing service you choose to use to determine how it uses this data.

Choice and control

You can use the Online Print Wizard to choose which pictures to send and which service to use to print your pictures. Some picture management applications might be able to help you remove stored personal information before sending pictures to be printed. You might also be able to edit the properties of the file to remove stored personal information. For more information about viewing or changing file properties, see Windows Help and Support.

Top of Page

Parental Controls

What this feature does

This feature helps parents to restrict and monitor the activities of their children on the computer. Restrictions can be placed to limit the games their children can play, what websites and web content they can view, when they can use the computer, and what applications they can run. In addition, logs can be created to record the child's usage, each activity the child attempts that is restricted by parental controls, and any changes made to those restrictions. To properly use this feature, only parents should be administrators of the computer, and children should not be granted administrative privileges.

Information collected, processed, or transmitted

Parental Controls settings that are used to determine which sites and activities to restrict or monitor are stored locally. The log is stored locally and contains information about a child's activity as well as any changes to parental controls settings for that child.

When web browsing restrictions are turned on, URLs that a child attempts to use are checked against the local Allow and

Block lists that can be created by an administrator. If the URL is not on one of these lists, then the URL is transmitted to Microsoft's Web Content Filter service to determine, if possible, the type of content offered by the website.

Use of information

URLs are used to try to determine the appropriate rating for sites that are not on local Allow and Block lists, and to block the site if necessary. URLs are also used to analyze and improve the ratings service. To help protect your privacy, the URLs are not stored with any information about the user or the computer from which the request came. Whether a site is blocked is determined locally based on the information returned by Microsoft's Web Content Filter Service and the locally stored Parental Controls settings. Microsoft does not use the information collected or transmitted by the Parental Controls feature to identify you or contact you.

Choice and control

Only users without administrative privileges can be monitored using Parental Controls. Administrators cannot be monitored and have full control of the settings and the log. Parental Controls are turned off by default. Only administrators may turn this feature on. Other users can view only the settings an administrator has applied to their own account. A monitored or restricted child will be notified by the presence of an icon in the Notification area that Parental Controls are turned on for their account.

Top of Page

Peer Name Resolution Service

What this feature does

Peer Name Resolution Service allows applications and services to register and to look up a remote application or service, and then get the associated IP address to enable communication with each other over the Internet or a network. A Peer Name is a unique set of alphanumeric characters (for example, 25028246da822ce8ba9a8135552e7a1bcaa50db6).

Information collected, processed, or transmitted

When you publish a Peer Name using the Peer Name Resolution Protocol (PNRP), the Peer Name Resolution Service publishes a hash of your Peer Name and associates it with your IP address. If an application you are running has published a Peer Name, any computer running the Peer Name Resolution Service can look up the published Peer Name to get your IP address, and then connect and communicate with your computer over the Internet or a network.

Use of information

PNRP information is used by other computers to locate and communicate directly with your computer, enabling peer-to-peer connectivity for services and applications. The information is registered on a Microsoft server so your computer can communicate with other PNRP clients outside your local subnet over the Internet. This information is periodically overwritten by other PNRP information. Microsoft does not use this information to identify you or contact you.

Choice and control

By default, the Peer Name Resolution Service is enabled but does not start running until an application needs to use it. To allow or prevent publishing and resolution of Peer Names from your computer, an administrator can enable or disable the Peer Name Resolution Protocol using Services in Administrative Tools, located under System and Maintenance in Control Panel. However, disabling the service might prevent some features of Windows, such as Windows Meeting Space, from functioning properly. For more information about Administrative Tools, see Windows Help and Support.

Top of Page

Plug and Play

What this feature does

Windows Plug and Play makes it easier to install hardware devices on your computer. When you plug in a Plug and Play device, Windows automatically installs compatible drivers, updates your computer to recognize the device, and allocates the system resources that your computer needs to work with the device. After you install a Plug and Play device, the driver is configured and loaded dynamically whenever you use the device, typically without requiring your input.

Information collected, processed, or transmitted

When you install a Plug and Play device, the Windows Update client contacts the online Windows Update service to find and download device drivers. The Windows Update client handles all of the communication between the computer and Windows Update. To learn more about the information collected by Windows Update and how it is used, see the Windows Update Privacy Statement.

Use of information

Plug and Play detects and manages Plug and Play devices, performing tasks such as: determining hardware resource requirements; locating appropriate device drivers; loading and unloading drivers; and, in conjunction with power management, handling stop and start processes for devices. When you install a Plug and Play device, the information that is sent to the online Windows Update service is used to download and install the appropriate device drivers.

Choice and control

Plug and Play is enabled by default. To prevent reliability problems, Plug and Play cannot be disabled. However, administrators can determine the search locations for drivers, or prevent users and computers from automatically accessing Windows Update.

Top of Page

Plug and Play Extensions

What this feature does

Plug and Play Extensions (PnP-X) provides the same experience for network-connected devices as Plug and Play does for devices that are connected directly to your computer. In addition, this feature allows your computer to discover and connect to devices on your local network (subnet), and it allows devices that support PnP-X to broadcast their presence on a subnet. After you install a PnP-X enabled device, the driver is configured and loaded dynamically whenever you use the device, typically without requiring your input.

Information collected, processed, or transmitted

P-X enabled devices may advertise their presence on the subnet by broadcasting data, such as the device's IP address and a unique identifier, over the subnet. Be aware that PnP-X supports a wide range of devices, including network drives and devices (such as digital cameras) that could contain personal information. Also, when you install a PnP-X enabled device, the Windows Update client contacts the online Windows Update service to find and download device drivers. The Windows Update client handles all of the communication between the computer and Windows Update. To learn more about the information collected by Windows Update and how it is used, see the Windows Update Privacy Statement.

Use of information

When you install a PnP-X enabled device, the information that is sent to the online Windows Update service is used to download and install the appropriate device drivers. Information sent over the subnet is used to identify the device and enable access to the features offered by the device.

Choice and control

Administrators can determine the search locations for drivers, or prevent users and computers from automatically accessing Windows Update. There is no facility for disabling PnP-X or for controlling which information is sent by a PnP-X enabled device once it is accessed across a network. Before attaching PnP-X enabled devices to your network, we recommend that you verify that your network is secure. For example, if you use a cable modem to connect to the Internet, consider installing a router that isolates your area of the network from that of other users on the network. Or, if you have a wireless network, we recommend that you turn on an authentication service such as Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA). For more information about helping to secure a wireless network, see Windows Help and Support.

Top of Page

Program Compatibility Assistant

What this feature does

If an incompatibility error is found with a program you attempt to run, Program Compatibility Assistant will try to help you resolve the compatibility issue. There are two types of programs that the feature can help with:

- **A known incompatible program:** If the program is on the list of known incompatible programs that is included in Windows Vista, the Program Compatibility Assistant starts. If the program is known to cause a serious problem, it will be blocked. Otherwise, Program Compatibility Assistant warns you about the incompatibility problem and offers you the option of running the program. In either case, the Program Compatibility Assistant offers the option of checking online for information or solutions.

- **A program that fails in a way that indicates incompatibility:** If a program fails in a way that is typical of incompatible programs, the Program Compatibility Assistant starts and offers you the option of running the program again with recommended compatibility settings. For example, the Program Compatibility Assistant will start if you attempt to install a program that requires Windows XP compatibility mode.

Information collected, processed, or

transmitted

The Program Compatibility Assistant works with the Microsoft Error Reporting Service to report incompatibility errors to Microsoft. Error reports may be generated that include information such as the program name, the needed compatibility settings, and your actions with the program so far. If you attempt to start a program on the list of known incompatible programs, an error report is created only when you select the option to check online for a solution. If the program fails in a way that indicates incompatibility, an error report is immediately generated. Unless you have previously consented to report problems automatically so you can check for solutions, you are asked if you want to send the error report. Microsoft does not use the information to identify you or contact you.

For more information about Windows error reports and your privacy, see the Privacy Statement for the Microsoft Error Reporting Service.

Use of information

Error reports are used to provide you with responses to problems that you report for your programs. Responses contain links, when available, to the program vendor's website so you can learn more about possible solutions. Error reports created due to program failures are used to try to determine which setting to adjust when you encounter application compatibility problems for the programs that you're running on this version of Windows.

Choice and control

You can choose if you want to use the Program Compatibility Assistant to report compatibility errors to Microsoft. Administrators can use Group Policy to disable the Program Compatibility Assistant or Windows error reporting to prevent data from being sent to Microsoft.

Top of Page

Program Properties — Compatibility Tab

What this feature does

If you have an application compatibility problem, you can use the Compatibility tab to make program settings adjustments to attempt to run the program successfully on this version of Windows.

Information collected, processed, or transmitted

When you apply compatibility settings using the Compatibility tab, a Windows error report is generated that contains the program name and the compatibility settings used. Unless you have previously consented to report problems automatically so you can check for solutions, you are asked if you want to send the error report. Microsoft does not use the information to identify you or contact you.

For more information about Windows error reports and your privacy, see the Privacy Statement for the Microsoft Error Reporting Service. For more information about the Compatibility tab, see the Windows Help and Support topic, "Make older programs run in this version of Windows".

Use of information

Information sent by the Compatibility tab to Microsoft is used to determine which setting to adjust when you encounter application compatibility problems for the programs that you're running on this version of Windows.

Choice and control

Administrators can use Group Policy to disable the Program Compatibility Tab or configure Windows error reporting settings to prevent data from being sent to Microsoft.

Top of Page

Program Compatibility Wizard

What this feature does

If you have an application compatibility problem, you can use the wizard to make adjustments to how a program works and attempt to run the programs successfully on this version of Windows.

Information collected, processed, or transmitted

If you choose to send them, the results of running the Program Compatibility Wizard, including settings and problems that were encountered with the application being installed, are sent to Microsoft as a Windows error report. Microsoft does not use the information to identify you or contact you.

For more information about Windows error reports and your privacy, see the Privacy Statement for the Microsoft Error Reporting Service. For more information about the Compatibility tab, see the Windows Help and Support topic, "Make older programs run in this version of Windows".

Use of information

Information sent by the Program Compatibility Wizard to Microsoft is used to try to determine which setting to adjust when you encounter application compatibility problems for the programs that you're running on this version of Windows.

Choice and control

You will be asked if you would like to send the information to Microsoft and may choose not to. Administrators can disable the Program Compatibility Wizard or prevent data from being sent to Microsoft using Group Policy.

Top of Page

Properties

What this feature does

Properties are a set of information that allows you to quickly search and organize your files. They can also be used by applications to perform application-specific tasks (for example, to correct the exposure of a picture). Some properties are intrinsic to the file (for example, the size of the file) while others may be specific to an application or device (for example, the settings of your camera when you took a picture). You can see the properties for your files and for some properties, you can choose the information that they contain. For example, you might want to change or remove keywords or comments before sharing your files with someone else.

Information collected, processed, or transmitted

The type of information collected will depend upon the type of file and the applications that use it. Examples of properties include file name, date modified, file size, author, keywords, and comments. Properties are stored in the file, and they move with the file if it is moved or copied to another location, such as a file share, or sent as an e-mail attachment.

Use of information

Properties can help you more quickly search and organize your files. They can also be used by applications to perform application-specific tasks (for example, to correct the exposure of a picture). Properties are not sent to Microsoft unless you choose to send a file to Microsoft.

Choice and control

You can edit or remove some properties for a file using the preview pane in Windows Explorer, or by right-clicking a file, and then clicking **Properties**. Some intrinsic properties, such as date modified, file size, file name, and some application-specific properties cannot be removed this way. For application-specific properties, you can edit or remove them only if the program used to generate the file supports these features. For more information about changing or removing file properties, see Windows Help and Support.

Top of Page

Registration

What this feature does

Registration of your Windows Vista software is optional and can be done at any time. You can register to get tips, creative hints, and other information that will help you get the most out of Windows Vista.

Information collected, processed, or transmitted

To complete the registration process, we will ask you to provide some information about yourself, such as your name, e-mail address, and country or region. In addition, we will automatically send some information about your computer, such as the version of Windows that you're running, type of computer hardware, and a portion of your product key.

Use of information

The information collected will be used to help us better understand your needs, and to provide you with information about Windows Vista. The partial product key information is used to identify the computer manufacturer and the channel you purchased your computer from. The partial product key cannot be used to uniquely identify your computer. For more information about the privacy of your registration information, including how to update it, read the Microsoft Online Privacy Statement on the Microsoft website.

Choice and control

You can access Windows Vista online registration in the Welcome Center under System and Maintenance in Control Panel. To update your registration information, follow the instructions for updating your profile that are provided in the Microsoft Online Privacy Statement at the Microsoft website.

Top of Page

Rights Management Services (RMS) Client

What this feature does

Rights Management Services (RMS) Client software is information protection technology that works with RMS enabled applications to help safeguard digital information from unauthorized use—both online and offline and inside and outside of a firewall. You can define how recipients can use the information contained in a file, such as who can open, modify, print, forward, or take other actions with the file. In order to create or view a file with restricted permissions, your computer must be running an RMS enabled application and have access to an RMS server.

Information collected, processed, or transmitted

RMS uses your e-mail address to identify you. Your e-mail address will be stored on your computer in use licenses and identity certificates created by an RMS server. Identity certificates and use licenses are transferred to and from RMS servers. If your computer is part of an enterprise or networked environment, the RMS server is typically owned by and located within the enterprise. If you are using Windows Live services, the server will be an RMS server at Microsoft. Your e-mail address is also stored on the RMS server. Information that is sent to Microsoft RMS servers is sent using Secure Socket Layer (SSL) protocol.

Use of information

The use license allows you to access protected information. The identity certificate is used to identify you to an RMS server, and it allows you to protect information and access protected information.

Choice and control

RMS Client features are not enabled by default and you can choose not to enable or use them. However, if you do not enable them, you will not be able to open files with restricted permissions.

Top of Page

Speech Recognizer

What this feature does

Microsoft Speech Recognizer for Windows provides speech recognition within Windows and any applications that choose to use it. Speech recognition by the Microsoft Speech Recognizer will increase in accuracy when adaptation is enabled. Adaptation increases speech recognition accuracy by learning how you speak, including the sounds and words you like to use, the relative frequency of your words, and the way you use grammar.

Microsoft Speech Recognizer also uses a User Lexicon. The User Lexicon contains a list of words and their pronunciations. When you choose to add a new word using the Speech Dictionary, or to add a new pronunciation to an existing word, the entry is saved in the User Lexicon. If you are a Tablet PC user, words that you add for handwriting recognition are also added to the User Lexicon.

Information collected, processed, or transmitted

When adaptation is enabled, text that you author in documents on your system is collected and stored, typically in three-word fragments, along with corrections that you make while using speech to dictate. Additionally, you may add specific words to your User Lexicon by using the Speech Dictionary.

This information is stored in your personal speech profile. Speech Profiles are stored for each user, and users are not able to access the profiles of other users on the computer. Administrators can access any profile on the computer. The information is not sent to Microsoft.

Use of information

Microsoft Speech Recognizer uses words from the User Lexicon during dictation. The Speech Recognizer also learns about your language use by analyzing text that you have authored. In addition, analysis is done on corrections you make while using speech to dictate, and probability weightings are determined for the words you use. This allows for more accurate speech recognition.

Choice and control

All users can enable or disable adaptation in the Speech

Recognition feature. Additionally, you may delete your speech profile (and most adaptation data) by using the advanced Speech Recognition options in Ease of Access in Control Panel. You can also use the **Change existing words** option in the Speech Dictionary to delete words that you've added to the User Lexicon. Deleting your Speech Profile does not delete your User Lexicon. If you use your user profile on other computers, any user-specific words you may have added might be stored on the other computer unless you delete them.

Top of Page

Trusted Platform Module (TPM) Services

What this feature does

The Trusted Platform Module (TPM) security hardware is a microchip built into some computers that, if present and initialized, enables your computer to take full advantage of advanced security features such as BitLocker Drive Encryption.

TPM Services provides a set of software components for security features that use version 1.2 of the TPM. TPM Services include TPM initialization and management tools, a driver, and a software layer that allows applications to share use of the TPM.

Information collected, processed, or transmitted

TPM Services include TPM initialization functionality to help you turn on and create an owner for the TPM. As part of the initialization process, you are asked to create a TPM owner password. To use your computer's TPM, you must create a TPM owner password. The TPM owner password helps ensure that only you have access to the administrative functions of the TPM. Saving the TPM owner password allows you to easily manage access to the TPM.

The TPM Initialization Wizard allows you to print your TPM owner password or save it to a file on a USB flash drive. A saved file contains authorization information for the TPM owner that is derived from the TPM owner password. The file also contains the computer name, operating system version, creation user, and creation date information to assist you in recognizing the file. In an enterprise, administrators can configure Group Policy to automatically save this TPM owner information to Active Directory Domain Services.

Each TPM has a unique cryptographic "endorsement key" that it uses to indicate its authenticity. The endorsement key may be created and stored in the TPM by your computer's manufacturer, or Windows may need to trigger creation of the endorsement key inside the TPM. The endorsement key is never fully exposed outside of the TPM, and once it has been created, it cannot be reset.

Once the TPM is initialized, applications can use the TPM to create and help secure additional unique cryptographic keys. For example, BitLocker Drive Encryption uses the TPM to help protect the key that encrypts the hard drive.

Use of information

If you choose to save the TPM owner password to a file, the additional computer and user information saved inside this file helps you to identify the matching computer and TPM. The TPM endorsement key is used by Windows only during TPM initialization to encrypt your TPM owner password before sending it to the TPM. Windows does not transmit cryptographic keys outside of your computer.

Choice and control

Once your computer's TPM is initialized, TPM Services enables an administrator to prevent access to selected TPM functionality through a command management feature. By default, Windows blocks TPM commands that might reveal personal information, as well as TPM commands that have been deprecated or deleted from previous versions of the hardware. This block list may be modified by an administrator.

You can choose to turn off the TPM at any time. Turning off the TPM prevents software on your computer from using the cryptographic capabilities of the TPM. You can also choose to clear the TPM and reset it to factory defaults. Clearing the TPM removes owner information and, with the exception of the endorsement key, all TPM-based keys or cryptographic data that applications may have created when the TPM was in use.

Top of Page

Update Root Certificates

What this feature does

When an application is presented with a certificate issued by a certification authority that is not directly trusted (a certificate that is not stored in a list of trusted certificates on your computer), the Update Root Certificates feature will contact the online Windows Update service to see if Microsoft has added the certification authority to its list of trusted authorities. If the certification authority has been added to the Microsoft list of trusted authorities, its certificate will automatically be added to the list of trusted certificates (certificate store) on your computer.

Information collected, processed, or transmitted

Update Root Certificates sends a request to the online Windows Update service that asks for the current list of root certification authorities in the Microsoft Root Certificate Program. If the untrusted certificate is named in the list, Update Root Certificates obtains that certificate from Windows Update and places it in the trusted certificate store on your computer. Microsoft does not use the information transferred during this process to identify you or contact you.

For more information about Windows Update and your privacy, read the Windows Update Privacy Statement.

Use of information

The information is used by Microsoft to update the trusted certificate store on your computer.

Choice and control

Update Root Certificates is enabled by default. To disable the Update Root Certificates on a computer, see Using Windows Vista: Controlling Communication with the Internet on the Microsoft TechNet website.

Additional information

If you are presented with a certificate issued by a root authority that is not directly trusted, and the Update Root Certificates component is not installed on your computer, you will be prevented from completing the action that required authentication. For example, you might be prevented from installing software, viewing an encrypted or digitally signed e-mail message, or using a browser to engage in a Secure Socket Layer (SSL) session.

Top of Page

UPnP Technology

What this feature does

UPnP technology provides peer-to-peer device control for network devices. UPnP technology enables discovery and control of devices and services through standards-based protocols.

Information collected, processed, or transmitted

Using the IP address that is provided by this feature in the discovery process, your computer can receive information from UPnP devices, including any changes in their status. If a UPnP device provides a uniform resource locator (URL), you can use a browser to access control features, information, or device-specific capabilities from the manufacturer.

Use of information

The information exchanged includes basic information about the devices and their services, and a URL that can be used to gather more information, such as device make, model, and serial number. Additionally, the information can include a list of devices and services, and URLs used for accessing features.

Choice and control

To allow or prevent discovery of UPnP devices on your network, you can enable or disable the Simple Service Discovery Protocol (SSDP) discovery service in Windows. Before allowing UPnP devices to communicate on your network, we recommend that you verify that your network is secured. For example, if you use a cable modem to connect to the Internet, consider installing a router that isolates your area of the network from that of your neighbors. Or, if you have a wireless network, we recommend that you turn on a secure authentication service such as Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA). For more information about helping to secure a wireless network, see Windows Help and Support.

Top of Page

Windows Anytime Upgrade

What this feature does

Windows Anytime Upgrade allows you to easily upgrade your version of Windows Vista by directing you to a participating merchant website where you can purchase the upgrade.

Information collected, processed, or transmitted

When you use Windows Anytime Upgrade, you will be sent to a Microsoft website. Some additional information will also be sent, including your current Windows Vista edition and country or region code, the version you would like to upgrade to, the vendor that your current operating system was purchased from, and the merchant that your upgrade request should be directed to.

Use of information

The information is used to connect you with the merchant and to help ensure that you can upgrade your computer to the correct version of Windows. The information is first sent to a Microsoft server, where it is used for auditing purposes, and then redirected to the appropriate participating merchant.

Choice and control

You can begin an upgrade at any time, or cancel the evaluation and purchase process at any time. Administrators can disable Windows Anytime Upgrade through Group Policy.

For more information about Windows Anytime Upgrade, see Windows Help and Support.

Top of Page

Windows Calendar

What this feature does

Windows Calendar offers you an easy way to manage appointments and tasks, and it allows you to publish any calendars you create so they may be shared with other users.

Information collected, processed, or transmitted

Information that you enter in your calendars is stored locally on your computer. If you choose to publish a calendar, the information will be exported to the host server of your choice and made available to any user who subscribes to your calendar on the host server. Subscribers will be able to view the summary information (or title) of your appointments. You can choose to share other information such as calendar notes, event titles, alarms, and tasks. Any updates that you make to your calendar information will be sent to all subscribers, if you choose.

Use of information

Your calendar helps you keep track of your appointments and tasks. Publishing your calendar information allows others to do the same. If you publish your calendar, we recommend that you do not enter personal information in your calendar that you do not want to other people to view.

Choice and control

You may choose whether to publish calendar notes, event titles, alarms, or tasks for each of your calendars. Once published, you may choose to automatically synchronize calendar updates for all subscribers to receive. You may choose to publish your calendar with password protection, limiting subscribers to only designated friends and family members who can access and view it. You can remove any of your published calendars from the host server at any time. The server used to host published calendars might be owned by your Internet Service Provider (ISP), or another third party. If you send information to a third-party, use of the information will be subject to the third-party's privacy practices.

Top of Page

Windows Collaboration Technologies

People Near Me

What this feature does

People Near Me is a service that identifies people nearby on your local network (subnet) who are using computers and allows those people to send you invitations for programs such as Windows Meeting Space. They can only invite you to participate in programs that are installed on your computer. To use People Near Me, you have to sign in to the service.

Information collected, processed, or transmitted

By default, your People Near Me display name, computer name, and IP address are visible to all people on your local network. If you choose to include it, your user account picture (the picture displayed on the Start menu) will also be visible. Programs using People Near Me might publish additional information that can be seen by other users.

Use of information

This information is not sent to or used by Microsoft. Only people on your local network (subnet) can see the information.

Choice and control

You can choose to automatically sign in and use People Near Me when you log on, or sign in each time you want to use the service. You can also choose your People Near Me display name and user account picture.

Windows Meeting Space

What this feature does

Windows Meeting Space helps you to more effectively collaborate with people in a meeting room or across the Internet. You can share files, stream your desktop or an application to others, and keep track of who is attending meetings. You can also create ad-hoc wireless networks to enable collaboration anytime or anywhere.

Information collected, processed, or transmitted

During Windows Meeting Space sessions, all participants will be able to see your People Near Me display name, IP address, and computer name, as well as your user tile, which is the picture normally displayed on the Windows Start screen.

Use of information

The information is used by other Windows Meeting Space participants to identify you. Only Windows Meeting Space participants can see the information. This information is not sent to or used by Microsoft.

Choice and control

You can choose the meetings that you want to participate in. You may also choose your People Near Me display name, user tile, and the files that you want to share with other participants. Your user tile can be excluded from sharing with others by clearing the option in the People Near Me Personal Settings dialog box. You are notified about who is participating in each Windows Meeting Space session that you participate in.

Top of Page

Windows Control Panel

What this feature does

Control Panel features the Search box which you can use to more easily search all tasks that are possible through Control Panel and find the right one for your needs.

Information collected, processed, or transmitted

If you choose to help improve Control Panel search results, the queries that you type into the Search box are sent to Microsoft. Microsoft does not use the information to identify you or contact you. Queries are sent to Microsoft only if they originate from the Search box within Control Panel. These queries are not sent from other implementations of the Search box.

Use of information

This information is used to help Microsoft provide better keywords for the tasks in Control Panel.

Choice and control

Windows does not send query information to Microsoft by default. You may opt-in to sending Control Panel Search box queries to Microsoft by consenting to send the information when you are asked. You can stop sending queries at any time by using the option provided in Control Panel when you perform a search.

Top of Page

Windows Help

Windows Online Help and Support

What this feature does

This feature, when turned on, allows you to search Windows Online Help and Support when you're connected to the

Internet, giving you the most up to date content available.

Information collected, processed, or transmitted

When you opt in to use Windows Online Help and Support, your search query is sent to Microsoft, as well as any rating or feedback you choose to provide about the help topics presented to you. Windows Online Help and Support does not intentionally collect any information that could be used to personally identify you. If you type such information into the search or feedback boxes, the information will be sent, but Microsoft does not use the information to identify you or contact you.

Use of information

Microsoft uses the information to return help topics in response to your search queries, to return the most relevant results, to develop new content, and to improve existing content.

Choice and control

The Windows Online Help and Support option is turned off by default. Results from Windows Online Help and Support will not be included when you use the help system until you turn on the option. You are given the opportunity to select Windows Online Help and Support the first time that you use Windows Help and Support. You may change your selection later by selecting **Settings** from the **Options** menu, or by selecting **Get online Help** from the toggle menu in the lower right corner of the Help window.

Help Experience Improvement Program

What this feature does

The Help Experience Improvement Program helps Microsoft identify trends in the way you use Help so that we can improve our search results and the relevancy of our content. We will use this information to improve your future experience with Windows Help and Support. You may only participate in the Help Experience Improvement Program if you also choose to opt in to use Windows Online Help and Support.

Information collected, processed, or transmitted

The Help Experience Improvement Program sends Microsoft information about the version of Windows that your computer is running and about how you use Windows Help and Support, including queries you enter when you search Windows Help and Support.

Use of information

The data collected is used to identify trends and usage patterns so that Microsoft can improve the quality of content we provide and the relevance of our search results. Microsoft does not use the information to contact you or identify you.

Choice and control

The Help Experience Improvement Program option is turned off by default. You will not be enrolled in the Help Experience Improvement Program until you turn the option on. To turn the feature on or off, select **Settings** from the **Options** menu, or select **Get online Help** from the toggle menu in the lower right corner of the Help window. Administrators may use Group Policy to prevent data from being sent to Microsoft, and to restrict this data to include only Help Experience Improvement Program information and search queries.

Top of Page

Windows Mail

What this feature does

Windows Mail provides you with an e-mail and newsgroup reader. It includes features such as inbox customization rules, offline synchronization, instant search, and junk and phishing mail filters. Windows Mail also includes the Communities service which displays information about newsgroup messages, such as ratings and rankings. If your newsgroup server administrators choose to support Communities, newsgroup messages will be displayed with these additional Communities features.

Information collected, processed, or transmitted

You must enter your e-mail account information and server name for Windows Mail to connect to your e-mail server. You may also provide your Display Name, which is then shown in the e-mail header to everyone you send e-mail to. This information is not sent to Microsoft unless you send an e-mail to the company or use a Microsoft e-mail service such as Windows Live Mail, Hotmail, or MSN Mail. Your email service provider will process the email you send or receive. Any use of that information by the email service provider will be subject to their privacy practices.

If you choose to enable Communities, each time you start Windows Mail, your newsgroup servers will be checked to see if they support the Communities features such as message ratings and rankings. To use advanced Communities features (such as the ability to rate and rank newsgroup postings), you must sign in with your Windows Live ID credentials. For more information about Windows Live ID, see the Microsoft Online Privacy Statement.

Windows Mail uses the Contacts folder in Windows Vista to store and organize your contacts. It does not send any information about your contacts to Microsoft.

Use of information

Your e-mail account information is used to establish a connection to your e-mail server and provide a name of your choice to your e-mail recipients. In addition, you will be able to use advanced Communities features in the Newsgroup reader if you sign in with your Windows Live ID.

Choice and control

If you do not want to provide Windows Mail with your e-mail account information or e-mail server name, you can use any other e-mail application to connect to your e-mail server. If you choose not to use Windows Mail for e-mail, the program will not collect any information. If you use Windows Mail, you can select and change your Display Name or choose not to use a Display Name. You can enable Communities the first time that you subscribe to any newsgroup, and you can stop using Communities at any time using the options provided in Windows Mail.

Top of Page

Windows Movie Maker

Project Properties Dialog Box

What this feature does

To help you identify and organize the movies you create, you can use the Project Properties dialog box to enter information about each movie, such as the movie title, author, description, rating, and copyright.

Information collected, processed, or transmitted

The information you enter into the Project Properties dialog box is not sent to Microsoft, but anyone who has access to your Windows Movie Maker project files or movie files could view the information.

Use of information

The Publish Movie feature, which guides you through the process of publishing your completed project as a movie to your computer or to a device, will save the information you entered in the Project Properties dialog box with the movie. This information might be displayed when you or someone else plays your movie in a media player.

Choice and control

You should only enter personal information in the Project Properties dialog box that you are willing to share with others when they are watching your published movies. You can choose not to include this information with your published movie by using the options provided in the Tools menu of

Windows Movie Maker.

Removing a Clip

What this feature does

A clip may be removed from a collections folder, storyboard, or timeline in Windows Movie Maker, or from Windows Photo Gallery. This removes the information that defines the clip, but does not remove the underlying digital media file.

Information collected, processed, or transmitted

Clip information contains the location and file name that was used to make the clip, the type of file, and media-specific information, such as duration, or date taken. If you delete a clip, this does not delete the digital media file that the clip points to.

Choice and control

Digital media files may be deleted using Windows Explorer.

Top of Page

Windows Print Spooler

What this feature does

The Windows print spooler is responsible for many of the functions that enable printing.

Information collected, processed, or transmitted

Print job data is collected and stored in a spool file in a spooler directory. Job cover data sent by printer drivers, such as the Microsoft Postscript Print Driver, can include user name, job name, and job size, and this data is stored with the spooled data in a shadow file in the spooler directory. This data is available to third-party applications via programmatic interfaces, and it can be transferred over various standard protocols. Print queue data is stored in the registry. Ports are also stored in the registry, and can be created or viewed by any user, including remote users, who are logged on to the computer to which the printer has been added. Installable components such as language monitors, drivers, port monitors, and print providers are also visible to any user, both remotely and locally, as long as they belong to the "Everyone" group. This information is not sent to Microsoft.

Use of information

The information is used to enable printing functionality in Windows. Job data is used to display status to the users, administrators, and management tools on the status of jobs being processed. The contents of the document being printed are available only to the document owner and system administrators.

Choice and control

You can disable the spooler service by using the Services Administrative Tool in Control Panel. However, if you do so, you will not be able to print. All users can write spool files by default, but only administrators have permissions to read and update spool files. Job cover data, which includes information such as user name, job name, and job size can be read by all users.

Top of Page

Windows Problem Reporting

What this feature does

Many Microsoft software programs, including Windows Vista, are designed to work with the Microsoft Error Reporting Service. If a problem occurs in one of these software programs, you are asked if you want to send a report so you can check for a solution. You can view the details of the report before sending it, although some files might not be in a readable format.

The Microsoft Error Reporting Service helps Microsoft and Windows partners diagnose problems in the software you use and provide solutions. Not all problems have solutions, but when solutions are available, they are offered as steps to solve a problem you’ve reported or as updates to install.

In Windows Vista, you can report problems automatically instead of having Windows ask for your consent each time a problem occurs. If you use automatic reporting, you are not typically prompted to review the information in a report before it is sent. However, no information is sent unless you (or your system administrator or network administrator) choose to report problems. You can choose to stop reporting problems at any time.

Information collected, processed, or transmitted

Windows problem reporting can collect information about problems that interrupt you while you work, and about errors that occur behind the scenes. Reports might unintentionally contain personal information, but Microsoft does not use the information to identify you or contact you. For example, a report that contains a snapshot of computer memory might include your name, part of a document you were working on, or data that you recently submitted to a website. If you are concerned that a report might contain personal or confidential information, you should not send the report. If a report is likely to contain this type of information, Windows will ask if you want to send it, even if you have turned on automatic reporting. This gives you the opportunity to review the report before sending it to Microsoft.

Reports that you have not yet sent to Microsoft, including files and data attached to those reports, may be stored on your computer until you have an opportunity to review and send them. Reports that you have already sent, including files and data attached to those reports, may also be stored on your computer.

For more information about what data may be contained in error reports, see the Privacy Statement for the Microsoft Error Reporting Service.

Use of information

Microsoft uses information about errors and problems to improve Windows and the software and hardware designed for use with Windows operating systems. Microsoft employees, contractors, vendors, and partners may be provided access to information collected by the reporting service. However, they may use the information only to repair or improve the products that they publish or manufacture. For more information about how error report data is used, see the Privacy Statement for the Microsoft Error Reporting Service.

Choice and control

To view your problem history, check for new solutions, or delete problem reports and solutions, go to Problem Reports and Solutions in Control Panel or see Windows Help and Support for more information.

Top of Page

Windows Terminal Services Client

Remote Desktop Connection

What this feature does

Windows Terminal Services Client software (Remote Desktop Connection) provides a way for you to establish a remote connection with a host computer that is running Windows Terminal Services.

Information collected, processed, or transmitted

Connection settings are stored in a Remote Desktop Protocol (RDP) file on your computer. These settings include the name of your domain and connection configuration settings, such as remote computer name, color-bit depth, enabled session devices, audio, and clipboard. Credentials for these connections, as well as Terminal Services Proxy credentials, are stored using Stored User Names and Passwords. A list of trusted Terminal Services Gateway server names is stored in the registry. This list is stored permanently unless it is deleted by an administrator, and is not shared with third parties or other Windows components. The information is not sent to Microsoft.

Use of information

Data is collected from your computer so you can connect to servers (remote computers running Windows Terminal Services) using your preferred settings. User name, password, and domain information are collected to allow you to save your connection settings and to enable you to double-click on an RDP file to launch a connection.

Choice and control

You can choose whether to use Remote Desktop Connection. If you use it, your RDP files contain information required to connect to a remote computer, including the options and settings that were configured when the file was automatically saved. You can customize RDP files, including files for connecting to the same computer with different settings. For more information about using Remote Desktop Connection, see Windows Help and Support.

Additional information

For more information about data that is stored in the RDP files, see the Microsoft Developer Network (MSDN) article, Win32_TSRemoteControlSetting, online. For more information about the Remote Desktop Connection, see Windows Help and Support.

Windows Remote Assistance

What this feature does

You can use Windows Remote Assistance to invite someone to connect to your computer and help you with a computer problem, even if that person isn't nearby. After connecting, the other person can view your computer screen and chat with you about what you both see. With your permission, your helper can use his or her mouse and keyboard to control your computer and show you how to fix a problem. You can also help someone else the same way.

Information collected, processed, or transmitted

Windows Remote Assistance creates an encrypted connection between the two computers over the Internet or the network that both computers are connected to. When someone uses Windows Remote Assistance to connect to your computer, that person can see your desktop, any open documents, and any visible private information. In addition, if you allow your helper to control your computer with his or her mouse and keyboard, that person can do things like delete files or change settings. No information is sent to Microsoft.

Use of information

The information is used to establish an encrypted connection and to provide your helper access to your desktop. No information is collected or sent to Microsoft. For more information on Windows Remote Assistance, see **Windows Remote Assistance: frequently asked questions** in Windows Help and Support.

Choice and control

Before you allow someone to connect to your computer, close any open programs or documents that you don't want your helper to see. Watch what your helper is doing. If at any time you feel uncomfortable about what that person is seeing or doing on your computer, press the ESC key to end the session.

Top of Page

Windows Time Service

What this feature does

The Windows Time service automatically synchronizes your computer's time with a reliable time server on a network to help improve security and performance across your network or in your organization.

Information collected, processed, or transmitted

The service sends information in the form of a network packet to a reliable time server. The connection uses industry standard Network Time Protocol (NTP). By default, this service synchronizes with time.Windows.com once a week. Information related to the service is stored in the Windows System event log in Event Viewer. The IP address of the time server is also stored in the Windows event log entries. Additionally, warning or error condition information related to the service is stored in the Windows System event log.

Use of information

Information is used by the Windows Time service to automatically synchronize the local computer's time with a reliable time server on the network.

Choice and control

The Windows Time service is turned on by default. You can turn this feature off or choose your preferred time source using the options provided in Date and Time in Control Panel. Turning off Windows Time Service has no direct effect on applications or other services, but without a reliable time source, the local computer’s clock may become unsynchronized with other computers on the network or Internet. Applications and services that depend on time may fail or stop working correctly if there is a significant time discrepancy between networked computers.

Top of Page