Microsoft

Quy

Để có thông tin cập nhập về các phương pháp xử lý dữ liệu của Microsoft, vui lòng xem lại Điều khoản về Quyền riêng tư của Microsoft. Tại đây, bạn cũng có thể tìm hiểu về các công cụ mới nhất mà chúng tôi cung cấp để truy nhập và kiểm soát dữ liệu của mình, cũng như cách liên hệ với chúng tôi nếu có thắc mắc về quyền riêng tư.

Điều khoản về Quyền riêng tư của Windows 7

Cập nhật lần cuối: **Tháng 2 năm 2011**

Điểm nổi bật | Điều khoản | Phần bổ sung

Trong trang này

Thông tin cá nhân

Lựa chọn của bạn

Việc sử dụng thông tin

Thông tin quan trọng

Cách liên hệ với chúng tôi

Những điểm nổi bật này bao gồm Tuyên bố về Quyền riêng tư của Windows 7 đầy đủ giải thích một số việc thu thập dữ liệu và sử dụng các thực tiễn của Windows 7 và tất cả các gói dịch vụ của Windows 7 ở cấp cao. Chúng bộ tập trung vào các tính năng liên lạc với Internet và không phải là mô tả hoàn chỉnh. Chúng không áp dụng cho trang web, sản phẩm hay dịch vụ trực tuyến hoặc ngoại tuyến của Microsoft.

Bảo mật và quyền riêng tư trực tuyến: câu hỏi thường gặp

Dành cho quản trị viên: Chi tiết về quản lý dữ liệu trong Windows Server 2008 R2 và Windows 7.

Thông tin cá nhân

- Các tính năng nhất định của Windows 7 có thể yêu cầu bạn cho phép thu thập hoặc sử

dụng dữ liệu cá nhân của bạn. Thông tin bổ sung về các tính năng này và cách chúng sử dụng thông tin cá nhân của bạn được mô tả trong Tuyên bố về Quyền riêng tư của Windows 7đầy đủ.

- Một số tính năng của Windows 7 cho phép bạn, dưới sự cho phép của bạn, chia sẻ thông tin cá nhân qua Internet.

- Nếu bạn chọn đăng ký phần mềm của mình thì bạn sẽ được yêu cầu cung cấp thông tin cá nhân.

- Các chi tiết bổ sung

Đầu trang

Lựa chọn của bạn

- Windows 7 cung cấp cho bạn nhiều cách để kiểm soát cách các tính năng của Windows 7 truyền thông tin qua Internet.

- Theo mặc định, một số tính năng kết nối với Internet được bật giúp Windows 7 hoạt động tốt hơn. Bạn có thể chọn vô hiệu hóa những tính năng. Để tìm hiểu thêm về những tính năng này, hãy xem Phần bổ sung về Tuyên bố về Quyền riêng tư của Windows 7đầy đủ.

- Các chi tiết bổ sung

Đầu trang

Việc sử dụng thông tin

- Chúng tôi sử dụng thông tin được thu thập để bật tính năng bạn đang sử dụng hoặc cung cấp các dịch vụ bạn yêu cầu. Chúng tôi cũng sử dụng thông tin này để cải tiến các sản phẩm và dịch vụ của mình. Nhằm giúp cung cấp các dịch vụ của mình, đôi khi chúng tôi cung cấp thông tin cho các công ty khác hoạt động nhân danh chúng tôi. Chỉ những công ty có công việc cần dùng thông tin mới được cung cấp quyền truy cập vào những thông tin đó. Những công ty này bắt buộc phải giữ bí mật thông tin này và không được phép sử dụng thông tin đó cho bất kỳ mục đích nào khác.

- Các chi tiết bổ sung

Đầu trang

Thông tin quan trọng

- Windows 7 yêu cầu kích hoạt để giảm thiểu việc sao chép trái phép phần mềm và giúp đảm bảo rằng các khách hàng của chúng tôi nhận được chất lượng phần mềm như họ kỳ vọng. Microsoft không sử dụng thông tin được thu thập qua quá trình kích hoạt để nhận dạng hay liên hệ với bạn.

- Tuyên bố đầy đủ về Tuyên bố về Quyền riêng tư của Windows 7 chứa các liên kết đến thông tin bổ sung về các tính năng cụ thể của Windows 7.

- Để biết thêm thông tin về cách giúp bảo vệ máy tính cá nhân, thông tin cá nhân và bảo vệ gia đình của bạn khi trực tuyến, hãy truy cập các tài nguyên về an toàn khi trực tuyếnđầy đủ.

Đầu trang

Cách liên hệ với chúng tôi

Để biết thêm thông tin về các thực tiễn về quyền riêng tư của chúng tôi, hãy đi đến Tuyên bố đầy đủ về Tuyên bố về Quyền riêng tư của Windows 7. Hoặc bạn có thể viết cho chúng tôi bằng cách sử dụng biểu mẫu webđầy đủ.

Đầu trang

Điều khoản về Quyền riêng tư của Windows 7

Microsoft

Quy

Để có thông tin cập nhập về các phương pháp xử lý dữ liệu của Microsoft, vui lòng xem lại Điều khoản về Quyền riêng tư của Microsoft. Tại đây, bạn cũng có thể tìm hiểu về các công cụ mới nhất mà chúng tôi cung cấp để truy nhập và kiểm soát dữ liệu của mình, cũng như cách liên hệ với chúng tôi nếu có thắc mắc về quyền riêng tư.

Điều khoản về Quyền riêng tư của Windows 7

Cập nhật lần cuối: **Tháng 2 năm 2011**

Trong trang này

Collection and use of your information

Collection and use of information about your computer

Security of your information

Changes to this privacy statement

For more information

This statement covers Windows 7 and all Windows 7 service packs. For information about software and services related to Windows and about prior releases of Windows, please refer to the list of privacy statements on the side of this page.

For information about specific features, please refer to the Windows 7 Privacy Supplement.

View the privacy notice highlights

Microsoft is committed to protecting your privacy, while delivering software that brings you the performance, power, and convenience you desire in your personal computing.

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 online or offline Microsoft sites, products, or services.

Collection and use of your information

The personal information we collect from you will be used by Microsoft and its controlled subsidiaries and affiliates to enable the features you use and provide the services or carry out the transactions you have requested or authorized. The information may also be used to analyze and improve Microsoft products and services.

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 for performing statistical analysis of our services. We will only provide those companies the personal information they need to deliver the service, and they are prohibited from using that information for any other purpose.

Microsoft may access or disclose information about you, including the content of your communications, in order to: (a) comply with the law or respond to lawful requests or legal process; (b) protect the rights or property of Microsoft or our customers, including the enforcement of our agreements or policies governing your use of the software; or (c) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of Microsoft employees, customers, or the public.

Information collected by or sent to Microsoft by Windows 7 may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries, or service providers maintain facilities. 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, the European Economic Area, and Switzerland.

Đầu trang

Collection and use of information about your computer

When you use software with Internet-enabled features, information about your computer ("standard computer information") is sent to the websites you visit and online services you use. Standard computer information typically includes information such as your IP address, operating system version,

browser version, and regional and language settings. In some cases, it may also include a hardware ID, which indicates the device manufacturer, device name, and version. If a particular feature or service sends information to Microsoft, standard computer information will be sent as well.

The privacy details for each Windows 7 feature in the supplemental privacy information listed on the side of this page describe what additional information is collected and how it is used.

Administrators can use Group Policy to modify many of the settings for the features described below. For more information see Using Windows 7 and Windows Server 2008 R2: Controlling Communication with the Internet.

Đầu trang

Security of your information

Microsoft is committed to helping protect 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.

Đầu trang

Changes to this privacy statement

We will occasionally update this privacy statement to reflect changes in our products, services, and customer feedback. When we post changes, 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 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.

Đầu trang

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 here.

Microsoft Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052
USA

Đầu trang

Điều khoản về Quyền riêng tư của Windows 7

Microsoft

Quy

Để có thông tin cập nhập về các phương pháp xử lý dữ liệu của Microsoft, vui lòng xem lại Điều khoản về Quyền riêng tư của Microsoft. Tại đây, bạn cũng có thể tìm hiểu về các công cụ mới nhất mà chúng tôi cung cấp để truy nhập và kiểm soát dữ liệu của mình, cũng như cách liên hệ với chúng tôi nếu có thắc mắc về quyền riêng tư.

Điều khoản về Quyền riêng tư của Windows 7

Cập nhật lần cuối: **Tháng 2 năm 2011**

Trong trang này

Activation
Audit
BitLocker Drive Encryption
Device Information Retrieval
Device Manager
Dynamic Update
Ease of Access Center
Event Viewer
Fax
Gadgets

Note that this page is a supplement to the Tuyên bố về Quyền riêng tư của Windows 7. In order to understand the data collection and use practices relevant for a particular feature or service, you should read the Windows 7 Privacy Statement and any applicable supplement.

Activation

What this feature does

Activation helps reduce software counterfeiting, which helps ensure that Microsoft customers receive the software quality 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. Some changes to your computer components or the software might require you to reactivate the software.

Information collected, processed, or transmitted

During activation, product key information is sent to Microsoft,

Games Folder

Handwriting recognition (Available only on Tablet PCs)

HomeGroup

Input Method Editor (IME)

Installation Improvement Program

Internet Printing

Location and Other Sensors

Microsoft Error Reporting Service

Network Awareness

Order Prints

Parental Controls

Plug and Play

Plug and Play Extensions

Program Compatibility Assistant

Program Properties Compatibility Tab

Properties

Remote Access Connections

such as:

- The Microsoft product code, which is a five-digit code that identifies the Windows 7 product you are activating.
- A channel ID or site code, which identifies where you obtained the Windows 7 product. For example, it identifies whether the product was sold at retail, is an evaluation copy, is subject to a volume licensing program, was pre-installed by the computer manufacturer, and so on.
- The date of installation.
- Information that helps confirm that the product key information has not been altered.

If you license Windows 7 on a subscription basis, information will also be sent about how your subscription works.

Activation also sends to Microsoft a number generated from the computer's hardware configuration. The number does not represent any personal information or information about the software. It cannot be used to determine the make or model of the computer and it cannot be 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 to confirm whether you are eligible for certain support programs. It is also 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 you do not have a valid license for the software, you will not be able to activate Windows.

Đầu trang

Remote App and Desktop Connections

Remote Desktop Connection

Rights Management Services (RMS) Client

Teredo Technology

Trusted Platform Module (TPM) Services

Update Root Certificates

UPnP™ Technology

Windows Anytime Upgrade

Windows Customer Experience Improvement Program (CEIP)

Windows Defender

Windows File Association

Windows Help

ReadyBoost

Windows Remote Assistance

Windows Speech Recognition

Windows Time Service

Audit

What this feature does

Audit allows an administrator to configure Windows to record operating system activity in a security log that 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, for example whether someone has logged on to the computer, created a new user account, changed a security policy, or opened a document, and to troubleshoot problems.

Information collected, processed, or transmitted

Administrators determine what information is collected, how long it is retained, and whether it is transmitted to other parties. The information might 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. You can configure Audit on your computer by going to Local Security Policy in Administrative Tools.

Đầu trang

BitLocker Drive Encryption

What this feature does

If BitLocker is included in your version of Windows 7, it protects your data by helping to prevent offline software attacks. Supported hard drives and removable drives can be encrypted with BitLocker. When BitLocker is enabled on a drive, it fully encrypts the entire contents of the drive.

Windows Troubleshooting

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 drive. During BitLocker setup, you can choose to print a recovery key, save it to a location on your network, or, with the exception of removable drives, save your recovery key to a USB flash drive.

When you encrypt a drive using a smart card, the public key and unique identifier for the smart card is stored on the drive in unencrypted form. This information can be used to locate the certification authority that was originally used to generate the smart card's encryption certificate.

If your computer is equipped with the Trusted Platform Module (TPM) version 1.2 or higher security hardware, BitLocker uses the TPM to provide hardware-enhanced data protection for the drive on which Windows is installed. 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 drive.

Use of information
Cryptographic keys and globally unique identifiers (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 turned off by default. You can turn BitLocker on or turn it off for a removable drive at any time by going to BitLocker Drive Encryption in Control Panel. An administrator can turn BitLocker on or off for all drives, including hard drives.

Đầu trang

Device Information Retrieval

What this feature does

Device Information Retrieval downloads information from Microsoft about your hardware devices such as the manufacturer, description, and a picture of the device, and displays it to you.

Information collected, processed, or transmitted

In order to retrieve relevant device information, this feature sends data to Microsoft, including your Device ID (for example, Hardware ID or Model ID of the device you are using), your locale, and the date that device information was last updated. The device information downloaded to your computer might include a model name, description, device manufacturer logo, and device-related tasks.

Use of information

The information collected is used to help download relevant device information. No information sent is used to identify or contact you.

Choice and control

If you choose the recommended settings during Windows 7 setup, you turn on Device Information Retrieval. You can turn this feature off by going to Devices and Printers in Control Panel. In Devices and Printers, right-click your computer icon, and then click **Device installation settings**. Select **No, let me choose what to do**, and click to clear the **Replace generic device icons with enhanced icons** check box.

Đầu trang

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, such as what printers and other devices you use, 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 Update Services Privacy Statement.

Use of information
The information collected is used to determine which updates apply to your computer hardware and to installed devices. 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.

Đầu trang

Dynamic Update

What this feature does
Dynamic Update enables Windows 7 to perform a one-time check with the Windows Update website to get the latest updates for your computer while Windows 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
To install compatible drivers, Dynamic Update sends information to Microsoft about your computer's hardware. The types of updates Dynamic Update can download to your computer include:

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

Use of information

Dynamic Update reports information about your computer's hardware to Microsoft to identify the correct drivers for your system. For more information about how information collected by Dynamic Update is used, see the Update Services Privacy Statement.

Choice and control

At the start of Windows 7 setup, you will be given the choice to use Dynamic Update.

Đầu trang

Ease of Access Center

What this feature does
The Ease of Access Center enables you to turn on accessibility options and settings to help you more easily interact with the computer.

Information collected, processed, or transmitted
If you use this feature, you will be asked to select appropriate statements from a series.

These statements include:

- Images and text on TV are difficult to see.
- Lighting conditions make it difficult to see images on my monitor.
- I do not use a keyboard.
- I am blind.
- I am deaf.
- I have a speech impairment.

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 available only to you and to administrators on your computer, and not to other users.

Use of information
A set of configuration recommendations are provided to you based on the statements that you choose.

Choice and control
You can choose which statements you would like to select by going to Ease of Access Center in Control Panel. You can alter your choices at any time. You can also choose which of the recommendations you want to configure on your computer.

Đầu trang

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, software, and security events on your computer. You can also get information from Microsoft about events in the event logs by clicking on the **Event Log Online Help** link.

Information collected, processed, or transmitted
Event logs contain event information generated by all users and the programs on the computer. By default, all users can view event log entries; however, administrators can choose to restrict access to event logs. 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.

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. 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 sent to Microsoft. Microsoft does not use this information to contact you or identify you. For events associated with third-party programs, the information will be sent to the location specified by the third-party publisher or

manufacturer. 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
Administrators can choose to restrict access to Event Viewer logs. Users who have full access to event viewer logs can clear them. Unless you have previously consented to sending event information automatically 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.

Đầu trang

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 for each identifier.

Use of information

Information entered in the sender dialog box is presented on the fax 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

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. By default, 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, and the TSID and CSID values.

Đầu trang

Gadgets

What this feature does

Gadgets are programs that run on the desktop and provide at-a-glance information, and easy access to frequently used tools.

Information collected, processed, or transmitted

Some gadgets, such as Currency, Stocks, and Weather, contact the Internet to collect information and might send additional information, such as a location for weather information.

Use of information

Information collected by Microsoft from Microsoft gadgets is used to provide functionality for the gadgets but is not used to identify or contact you. If you use a non-Microsoft gadget, use of the information will be subject to the gadget provider’s privacy practices.

Choice and control

Certain gadgets, such as Weather, might be pre-configured to contact the Internet when you first use them. However, you might be able to configure or close them later by going to Desktop Gadgets in Control Panel.

Đầu trang

Games Folder

What this feature does

The Games folder lists games installed on your computer, giving you a single place to view and launch your games. The Games folder can also download additional information about games such as box art, publisher information, performance evaluations, and

parental control ratings.

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 information from Microsoft about the games you have installed. To do this, information including game identification numbers will be sent to Microsoft.

You can also choose to check for updates to some games by right-clicking the game icon and selecting **Scan online for Update**. Game version details and game identification numbers will be sent to Microsoft, and you will be notified of any updates that are available. You may choose to have Windows automatically scan and notify you about game updates from the options menu.

Some games, such as Internet Backgammon and Internet Spades, include a feature that will match you with players from around the world. If you choose to "Play," standard computer information and a GUID is sent to Microsoft to provide game play. No information collected is used to identify or contact you.

Use of information
The information sent to Microsoft is used to retrieve information for the games that you've installed. Microsoft does not use the information to identify you or contact you.

Choice and control
You can turn the information collection or the tracking features of the Games folder on or off. You can choose to retrieve and display game information and to track game playing times from the options menu. You can disable these features at any time by returning to the options menu. If you choose to quit an Internet game that comes with Windows 7, no information will be transferred to Microsoft.

Đầu trang

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 and external tablets. This feature collects data about the words that you use and how you write them. Automatic learning is enabled by default so that the handwriting recognition software can 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. 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 available only to you and to administrators on your computer, not to other users.

The information collected includes:

- Text from messages you compose and calendar entries you create by using e-mail programs such as Microsoft Office Outlook 2007 or Windows Live Mail, including any messages that you have already sent.
- Text that you type in your browser's 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 may collect additional information in some languages. For more information 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, and enables text prediction, suggesting words as you type on a soft keyboard.

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. No information is sent to Microsoft.

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 list of recently corrected handwriting samples is stored in memory. You can choose to send these handwriting samples to Microsoft. No personal information is intentionally collected; however the samples you choose to send may include personal information. For each report, you can also choose to send a comment about the errors. Microsoft does not use collected information to identify you or contact you.

Use of information

If you choose to send a report, it will be used to improve future versions of the Microsoft handwriting recognition software. No information is sent to Microsoft unless you choose to send it.

Choice and control

You can select which recognition errors you would like to report. You can initiate a report using the Handwriting Recognition Error Reporting tool while using the Tablet Input Panel. The Handwriting Recognition Error Reporting tool will also open when you select an alternate recognition after inking on a Tablet PC or another device. You can select each handwriting sample to be included in the report and review the report before sending it to Microsoft. No reports are sent automatically.

Personalization Training

What this feature does

Personalization training allows you to train the handwriting recognition software to better recognize your writing styles.

Information collected, processed, or transmitted

When you use Personalization Training, your handwriting samples are stored in memory. You can choose to send these handwriting samples to Microsoft. 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 or contact you.

Use of information
If you choose to send your handwriting samples to Microsoft, they are used to improve future versions of the Microsoft handwriting recognition software.

Choice and control
At the end of every training session you have the choice to send handwriting samples to Microsoft. No data is shared with Microsoft if you select **Don't send ink samples**.

Đầu trang

HomeGroup

What this feature does
A HomeGroup allows you to easily link Windows 7 computers on your home network so that you can share pictures, music, videos, documents, and devices. It also makes them ready to stream media to devices on your home network such as a media extender. You can help protect your HomeGroup with a password, and you can choose what you want to share.

Information collected, processed, or transmitted
In a HomeGroup, files such as pictures, videos, music, and documents are shared by default. Information such as user names is also shared with all users and computers within the HomeGroup.

Use of information
The information collected allows computers in your HomeGroup to understand who to share content with and how to present it. No information is sent to Microsoft.

Choice and control
You have the ability to add or remove computers from your HomeGroup and decide what is shared with other HomeGroup members. You can set or change your password at any time. You can create a HomeGroup and manage its settings by going to Network and Sharing Center in Control Panel.

Đầu trang

Input Method Editor (IME)

IME Learning

What this feature does

Microsoft Input Method Editors (IMEs) are 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.

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 is on by default but can be disabled by turning off the IME feature. In the Japanese IME, the learning feature can also be configured not to write to the user dictionary. You can also delete the contents of 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. These reports may include personal information, for example if you add personal names using word registration, 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

Microsoft uses the information to help improve input editing.

Choice and control
Each time you create a word registration report, 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.

Đầu trang

Installation Improvement Program

What this feature does
This feature sends a single report to Microsoft containing basic information about your computer and how you installed Windows 7. Microsoft uses 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.

If you choose to participate in the Installation Improvement Program, 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 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 and our partners use the report to improve our software. We use the GUID to correlate this data with data collected by the Windows Customer Experience Improvement Program (CEIP), a program you can choose to participate in when you are using Windows 7. 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 one hundred times and one hundred customers experiencing the same problem once. Microsoft does not use the information collected by the Installation Improvement Program to identify you or contact you.

Choice and control
You can choose to participate in this program when you install Windows 7 by selecting the **I want to help make Windows installation better** check box.

For more information, see the Windows Customer Experience Improvement Program (below).

Đầu trang

Internet Printing

What this feature does
Internet printing makes it possible for computers running Windows 7 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). Because the print job is unencrypted, it might be possible for others to see the content being sent. Once you are connected, you are presented with a list of available printers. If your computer does not have a print driver for your selected printer, you can choose to download a driver from the print server.

Use of information
The information collected enables you to print using remote printers. 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. 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 going to Programs and Features in Control Panel, and then selecting **Turn Windows features on or off**.

Đầu trang

Location and Other Sensors

What this feature does

Location and Other Sensors allows programs to access sensors through Windows. Sensors are hardware and software that can detect information such as your current location or the amount of light around your computer. This feature does not prevent or control programs from accessing sensors without using Location and Other Sensors. For example, some sensors may send sensor information directly to applications.

Information collected, processed, or transmitted

A sensor may provide personal information, such as the location of your computer, to any program on your computer. When you enable sensor access, any program on your computer can access sensor information and might transmit this information off your computer.

Use of information

Location and Other Sensors allows you to choose which sensors are accessible through this Windows 7 feature. No information is automatically sent to Microsoft by Locations and Other Sensors. If you choose to enable a sensor, any program on your computer could transmit sensor information off your computer.

Choice and control

You can choose whether Windows provides sensors information to programs and choose which users have that access. You can access these settings by going to Location and Other Sensors in Control Panel. This does not affect whether programs can access sensor information that is not provided through this Windows feature. For more information on controlling sensors and how sensors may affect your privacy, see Windows Help and Support.

Đầu trang

Microsoft Error Reporting Service

What this feature does

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. To help prevent problems and make software more reliable, some solutions are also included in service packs and future versions of the software.

The Microsoft Error Reporting Service also provides Setup Repair, an error reporting service that may run during Windows setup if a problem occurs.

Information collected, processed, or transmitted

Many Microsoft software programs, including Windows 7, are designed to work with the reporting service. If a problem occurs in one of these software programs, you might be asked if you want to report it. If you host virtual machines using a Windows operating system, reports generated by the Windows operating system for the Microsoft Error Reporting Service might include information about virtual machines.

The reporting service collects the information that is useful for diagnosing and solving the problem that has occurred, such as:

- Where the problem happened in the software or hardware
- The type or severity of the problem
- Files that help describe the problem
- Basic software and hardware information
- Possible software performance and compatibility problems

These reports might unintentionally contain personal information. For example, a report that contains a snapshot of computer memory might also include your name, part of a document you were working on, or data that you recently submitted to a website. If a report is likely to contain this type of information, Windows will ask if you want to send this information, even if you have enabled automatic reporting through the "Recommended settings"

option in setup, or in Control Panel. This gives you the opportunity to review the report before sending it to Microsoft. Reports including files and data might be stored on your computer until you have an opportunity to review and send them, or after they have been sent.

If an error report contains personal information, Microsoft does not use the information to identify you or contact you. In addition, if you enable automatic reporting through the "Recommended settings" option in setup, or in the Control Panel, the reporting service will send basic information about where problems occur automatically, but these reports will not have the details described above.

After you send a report, the reporting service might ask you for more information about the error you experienced. If you choose to provide your phone number or e-mail address in this information, your error report will be personally identifiable. Microsoft might contact you to request additional information to help solve the problem you reported.

The Microsoft Error Reporting Service generates a globally unique identifier (GUID) that is stored on your computer and sent with error reports to uniquely identify your computer. The GUID is a randomly generated number; it does not contain any personal information and is not used to identify you. 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 one hundred customers experiencing the same problem once.

Use of information
Microsoft uses information about errors and problems to improve Microsoft products and services as well as third-party software and hardware designed for use with these products and services. Microsoft employees, contractors, vendors, and partners might be provided access to information collected by the reporting service. However, they will use the information only to repair or improve Microsoft products and services and third-party software and hardware designed for use with Microsoft products and services.

Microsoft might share aggregate information about errors and

problems. Microsoft uses aggregate information for statistical analysis. Aggregate information does not contain specific information from individual reports, nor does it include any personal or confidential information that might have been collected from a report.

Choice and control
If you choose the recommended settings during Windows 7 setup, you turn on automatic checking for solutions, which will send basic error reports and look for solutions to the problems reported. If you use automatic checking, you are not typically prompted to send basic information about errors to Microsoft. If a more detailed error report is required, you will be prompted to review it. You can change this setting at any time by going to Action Center in Control Panel.

For more information, see the Privacy Statement for the Microsoft Error Reporting Service.

Đầu trang

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, network name, and gateway address of networks that your computer connects to. The Network Awareness feature makes the connectivity information available to programs on your computer that might require the information to function properly.

Information collected, processed, or transmitted
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. Your network connectivity status may be determined by attempts to connect to a Microsoft server designed for this purpose.

Use of information
Other than the standard computer information sent to the Microsoft server during network connectivity checks, information is not sent to Microsoft, but it is made available to programs on your

computer that request 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 Services in Administrative Tools. Disabling them is not recommended because that will prevent some Windows features from functioning correctly.

Đầu trang

Order Prints

What this feature does
Order Prints 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 digital photos are sent over the Internet to the service that you selected. The full file locations of the digital pictures that you select are 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 programs and Windows Explorer. For more information, see Properties (below).

After you select an online photo printing service within the Order Prints feature, you will be redirected to its website shown within the Order Prints window. Information you enter on the online photo printing services website is transmitted to the service.

Use of information
The information stored in the digital picture files by the camera might 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 programs might be used by the online photo printing service to print as captions on the front or back of the print copy. The online photo printing services' use of this information, and other information you provide to the services, such as information you enter on its website, will be subject to their privacy practices.

Choice and control
You can use Order Prints to choose which pictures to send and which service to use to print your pictures. Some picture management programs 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.

Đầu trang

Parental Controls

What this feature does
This feature helps parents restrict and monitor the activities of their children on the computer. Restrictions can be placed to limit the games their children can play, and what programs they can run. 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 and the activity log are stored locally. The Parental Controls activity log contains information about a child's activity as well as any changes to parental controls settings for that child.

Use of information
Parental Controls settings are used to determine which activities to restrict or monitor. No information is sent to Microsoft.

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. You can access parental controls by going to Parental Controls in Control Panel.

Đầu trang

Plug and Play

What this feature does

Windows Plug and Play makes it easier to install hardware devices on your computer. When you connect 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 Update Services 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 help avoid 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.

Đầu trang

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, and it allows devices that support PnP-X to broadcast their presence on a local network. After you install a PnP-X enabled device, the driver is configured and loaded whenever you use the device, typically without requiring your input.

Information collected, processed, or transmitted

PnP-X enabled devices may advertise their presence on the local network by broadcasting data, such as the device's IP address and a GUID, over the local network. PnP-X supports a wide range of devices, including network drives and devices (such as digital cameras) that could contain personal information. 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 Update Services 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, install, and manage the appropriate device drivers. Information sent over the local network 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 information about helping to secure a network, see Windows Help and Support.

Đầu trang

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 that is included in Windows 7 of known incompatible programs, 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, programs that fail because they require a specific screen resolution might be able to run on your computer even if you use a different screen resolution.

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 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

The dialog that notifies you of the error lets you choose if you want to use the Program Compatibility Assistant to report compatibility errors to Microsoft.

Đầu trang

Program Properties Compatibility Tab

What this feature does
If you have an application compatibility problem, you can use the Compatibility tab of the program properties window to make program setting adjustments that might allow the program to run successfully on Windows 7.

Information collected, processed, or transmitted
When you apply compatibility settings using the Compatibility tab, Microsoft Error Reporting generates a report that contains the program name and the compatibility settings used. Unless you have 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 Microsoft Error Reporting and your privacy, see Microsoft Error Reporting Service.

Use of information
Information sent by the Compatibility tab to Microsoft is used to determine and find solutions for compatibility problems for the programs that you're running on this version of Windows.

Choice and control
To learn how to control whether reports are sent to Microsoft, see Microsoft Error Reporting Service.

Đầu trang

Properties

What this feature does
Properties are file information that allow you to quickly search and organize your files. Some properties are intrinsic to the file (for example, the size of the file) while others may be specific to a program or device (for example, the settings of your camera when you took a photo or the location of the photo).

Information collected, processed, or transmitted
The type of information stored will depend upon the type of file and the programs 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 programs to perform program-specific tasks. No information is sent 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 program-specific properties

cannot be removed this way. For program-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.

Đầu trang

Remote Access Connections

What this feature does

A Remote Access Connections component, Dial-up Networking, allows you to access the Internet using a dial-up modem or broadband technology, such as a cable modem or a 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 components collect information from your computer such as your user name, password, and domain name. This information is sent to the system that you are attempting to connect with. No information is sent to Microsoft. To help protect your privacy and the security of your computer, security-related information such as your user name and password are encrypted and stored on your computer.

Use of information

Dialer information is used to help your computer connect to the Internet. No information is sent to Microsoft.

Choice and control

For non-command-line dialers, you can choose to save your password by checking **Save this user name and password**, and can clear that option at any time to delete the previously saved password from the dialer. Since this option is turned off by default,

you might be prompted to provide your password to connect to the Internet or a network. For command-line dialers like rasdial, there is no option to save your password.

Đầu trang

Remote App and Desktop Connections

What this feature does

The RemoteApp and Desktop Connections feature lets you access programs and desktops on remote computers that have been published online for remote access.

Information collected, processed, or transmitted

When you enable a connection, configuration files are downloaded to your computer from the remote URL you specify. These configuration files link programs and desktops on remote computers so that you can run them from your computer. Your computer will automatically check for and download updates to these configuration files periodically. These programs run on remote computers and information you enter into the programs is transmitted across the network to remote computers.

Use of information

Updates to RemoteApp and Desktop Connections configuration files may include settings changes including providing you with access to new programs; however new programs will run only if you choose to run them. This feature also sends information to the remote computers on which the remote programs run. The use of this data by the remote programs is subject to the privacy policies of the programs' manufacturers and the remote computers' administrators. Unless, you use the RemoteApp and Desktop Connections feature to access programs and desktops at Microsoft, no information is sent to Microsoft.

Choice and control

You can choose whether to use RemoteApp and Desktop Connections. You can add or remove RemoteApp and Desktop connections by going to RemoteApp and Desktop Connections in Control Panel. You can add a new connection by clicking **Set up a new connection with RemoteApp and Desktop Connections**, and entering a Connection URL in the dialog. You

can remove a connection and its connection files by clicking **Remove** on the connections description dialog. If you disconnect a connection without closing all open applications, these applications will remain open on the remote computer. RemoteApp and Desktop connections are not shown in the Add or remove programs list in Control Panel. For more information on RemoteApp and Desktop Connections, see Windows Help and Support.

Đầu trang

Remote Desktop Connection

What this feature does
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
Remote Desktop 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, user name, display information, local device information, audio information, clipboard, connection settings, and remote program names.

Credentials for these connections, as well as Terminal Services Proxy credentials, are stored using the Credential Manager. 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 sent to Microsoft.

Use of information
Information collected by this feature allows you to connect to 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 an RDP file to launch a connection. No information is sent to Microsoft.

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. To modify saved credentials, go to Credential Manager in Control Panel. For more information about using Remote Desktop Connection, see Windows Help and Support.

Đầu trang

Rights Management Services (RMS) Client

What this feature does

Rights Management Services (RMS) Client software is information protection technology that works with RMS-enabled programs to help safeguard digital information from unauthorized use. You can define how recipients use the information contained in a file, such as who can open, modify, print, 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 program 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. Your e-mail address is also stored on the RMS server. 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 RMS services, the server will be an RMS server at Microsoft. Information that is sent to Microsoft RMS servers is sent in an encrypted form.

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 features must be enabled through an RMS-capable program

and are not enabled by default. 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.

Đầu trang

Teredo Technology

What this feature does

Teredo Technology (Teredo) allows computers and networks to communicate over multiple networking protocols.

Information collected, processed, or transmitted

Each time you start your computer, if you need, to connect to Internet Protocol version 6 (IPv6), Teredo will attempt to locate a public IPv6 Internet service on the Internet. If you use a program that requires Teredo to use IPv6 connectivity, or if you configure your firewall to always enable IPv6 connectivity, then Teredo will periodically contact the Microsoft Teredo service over the Internet. The only information sent to Microsoft is standard computer information and the name of the service requested (for example teredo.ipv6.microsoft.com).

Use of information

The information sent from your computer by Teredo is used to determine if your computer is connected to the Internet and if it can locate a public IPv6 service. Once the service is located, information is sent to maintain a connection with the 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.

Đầu trang

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.

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.

Each TPM has a unique cryptographic endorsement key that it uses to indicate its authenticity. The endorsement key can be created and stored in the TPM by your computer's manufacturer, or Windows 7 might 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, programs 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 are no longer used in current 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 programs might have created when the TPM was in use.

Đầu trang

Update Root Certificates

What this feature does

The Update Root Certificates feature contacts the online Windows Update service to see if Microsoft has added a certification authority to its list of trusted authorities, but only when a program 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). 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 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 on the list, Update Root Certificates obtains that certificate from Windows Update and places it in the trusted certificate store on your computer. The information transferred includes the names and cryptographic hashes of root certificates. Microsoft does not use this information to identify you or contact you.

For more information about Windows Update and your privacy,

read the Update Services Privacy Statement.

Use of information
The information is used by Microsoft to update the list of trusted certificates on your computer.

Choice and control
Update Root Certificates is enabled by default. Administrators can configure Group Policy to disable the Update Root Certificates on a computer.

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 an encrypted session.

Đầu trang

UPnP™ Technology

What this feature does
UPnP technology provides peer-to-peer device control for network devices. UPnP technology helps find devices and services on networks and lets you control them, all through standards-based protocols.

Information collected, processed, or transmitted
If UPnP technology finds UPnP devices on your network, your computer can receive information from the devices, including any changes in their status. If a UPnP device provides a URL, you can use a browser to access control features, information, or device-specific capabilities from the manufacturer. Appropriately configured devices may also allow access to information stored on the device, including music, pictures, videos, and documents.

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 might include a list of devices and

services, and URLs used for accessing features. For applications that have permission to access UPnP devices, appropriately configured devices can send information stored on the device to the application, including music, pictures, videos, and documents. Some applications might have the capability to capture unencrypted streams and make a copy of the information stored on the device.

Choice and control

To allow or prevent discovery of UPnP devices on your network, you can enable or disable network discovery by going to the Network and Sharing Center in Control Panel and clicking **Change advanced sharing settings**. By default, UPnP technology is enabled if you configure your computer to join a Home network, but disabled if you select a Work or Public network. For more information about network discovery, see Windows Help and Support.

Before allowing UPnP devices to communicate on your network, we recommend that you verify that your network is secure. For information about helping to secure a wireless network, see Windows Help and Support.

Đầu trang

Windows Anytime Upgrade

What this feature does

Windows Anytime Upgrade allows you to easily upgrade your version of Windows 7 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 7 edition, 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.

When your version of Windows 7 is upgraded, updates may be available from Windows Update. As part of Windows Anytime

Upgrade, these updates will be downloaded and installed on your computer in accordance with your Windows Update settings. To learn more about the information collected by Windows Update and how it is used, see the Update Services Privacy Statement.

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 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.

Đầu trang

Windows Customer Experience Improvement Program (CEIP)

What this feature does
If you choose to participate in Windows CEIP, Microsoft collects basic information about how you use your programs, your computer, connected devices, and Windows 7. We also collect information about how each is set up and performing. When you participate, CEIP will also periodically download a file to collect information about problems you might have with Windows. CEIP reports are sent to Microsoft to help improve the features our customers use most often and create solutions to common problems. Microsoft does not use any collected information to identify you or contact you.

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 frequently you launch programs, 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 7 setup experience.

This information is sent to Microsoft when you are connected to the Internet. CEIP reports do not intentionally contain contact information, such as your name, address, or phone number; however, some reports might 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 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; it does not contain any personal information and is not used to identify you.

CEIP will also periodically download a file to collect information about problems you might have with Windows. This file allows Windows to collect additional information to help create solutions

for common problems.

Use of information
Microsoft uses CEIP information to improve our software. We might also share CEIP information with Microsoft partners so they can improve their software, but the information cannot be used to identify you. 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 one hundred customers experiencing the same problem once. Microsoft does not use the information collected by CEIP to identify you or contact you.

Choice and control
If you choose the recommended settings during Windows 7 setup, you turn on Windows CEIP. If you choose to participate, CEIP will collect the information described above for all users on your computer. Administrators can turn CEIP on or off by going to Action Center in Control Panel and selecting "Change Customer Experience Improvement Program settings."

For more information, see Microsoft Customer Experience Improvement Program Frequently Asked Questions.

Đầu trang

Windows Defender

What this feature does
Windows Defender looks for malware and other potentially unwanted software on your computer. It offers two ways to help keep malware and other potentially unwanted software from infecting your computer:

- **Real-time protection.** Windows Defender alerts you when malware or potentially unwanted software attempts to install or run on your computer. It also alerts you when programs attempt to change important Windows settings.

- **Scanning options.** You can use Windows Defender to scan for malware and other potentially unwanted software that might be installed on your computer, to schedule scans on a

regular basis, and to automatically remove any malicious software that is detected during a scan.

If you choose the recommended settings during Windows 7 setup, you turn on Windows Defender real-time protection and automatic scanning. Windows Defender will automatically download and install updated definitions before scanning, and then remove software that causes a severe or high alert level detected during the scan. You can change this setting at any time by using the options provided in Windows Defender.

Microsoft SpyNet Feature

What this feature does

The Microsoft SpyNet anti-malware community is a voluntary, worldwide community including Windows Defender users. Through Microsoft SpyNet, users can report malware and other forms of potentially unwanted software to Microsoft. When you set up Windows 7, you can choose to join Microsoft SpyNet. If you choose to join, reports about malware and potentially unwanted software are sent to Microsoft. The type of information that is sent in reports depends on your level of Microsoft SpyNet membership.

Information collected, processed, or transmitted

Microsoft SpyNet reports include information about the files or programs in question, such as file names, cryptographic hash, vendor, size, and date stamps. In addition, Microsoft SpyNet might collect full URLs to indicate the origin of the file, which might occasionally contain personal information such as search terms or data entered in forms. Reports might also include the actions that you applied when Windows Defender notified you that software was detected. Microsoft SpyNet reports include this information to help Microsoft gauge the effectiveness of Windows Defender's ability to detect and remove malicious and potentially unwanted software.

Reports are automatically sent to Microsoft when:

- Windows Defender detects software or changes to your computer by software that have not yet been analyzed for risks.
- You apply actions to software that Windows Defender has

detected.

- Windows Defender completes a scheduled scan and automatically applies actions to software that it detects, according to your settings.

Microsoft SpyNet might unintentionally collect personal information. To the extent that Microsoft SpyNet collects any personal information, Microsoft does not use the information to identify you or contact you.

You can join Microsoft SpyNet with a basic or an advanced membership. If you choose the recommended settings during Windows setup, you join with a basic membership. Basic member reports contain the information described above. Advanced member reports are more comprehensive and might occasionally contain personal information from, for example, file paths and partial memory dumps. These reports, along with reports from other Windows Defender users who are participating in Microsoft SpyNet, help our researchers discover new threats more rapidly. Malware definitions are then created for programs that meet the analysis criteria, and the updated definitions are made available to all users through Windows Update.

If you join Microsoft SpyNet with a basic or an advanced membership, Microsoft might request a Sample Submission report. This report contains specific files from your computer that Microsoft suspects might be potentially unwanted software. The report is used for further analysis. You will be asked each time if you want to send this Sample Submission report to Microsoft.

To help protect your privacy, reports that are sent to Microsoft are encrypted.

Use of information
Microsoft SpyNet reports are used to improve Microsoft software and services. The reports might also be used for statistical or other testing or analytical purposes, and for generating definitions. Only Microsoft employees, contractors, partners, and vendors who have a business need to use the reports are provided access to them.

Choice and control
You can join or leave Microsoft SpyNet or change your

membership level at any time.

You can turn automatic scanning on or off and change the frequency and type of scans. You can also choose which actions are automatically applied to software that Windows Defender detects during a scheduled scan.

You can change your Microsoft SpyNet membership or settings by using the Tools menu in Windows Defender.

History Feature

What this feature does
This feature provides a list of all programs on your computer that Windows Defender detects and the actions that were taken when the programs were detected.

In addition, you can view a list of programs that Windows Defender does not monitor while they are running on your computer (Allowed items). You can also view programs that Windows Defender prevents from running until you choose to remove them or allow them to run again (Quarantined items).

Information collected, processed, or transmitted
The list of software that Windows Defender detects, the actions that you and other users take, and the actions that Windows Defender takes automatically are stored on your computer. All users can view the history in Windows Defender to see malware and other potentially unwanted software that has attempted to install itself or run on the computer, or that has been allowed to run by another user. For example, if you learn about a new malware threat, you can check the history to see if Windows Defender has prevented it from infecting your computer. The History Feature does not send data to Microsoft.

Choice and control
History lists can be deleted by an administrator.

Đầu trang

Windows File Association

What this feature does
Windows File Association helps users associate file types with specific programs. If you try to open a file type that does not have

a program associated with it, Windows will ask if you want to use Windows File Association to find a program for the file. If you choose to use the service, it will send the file type extension to Microsoft. Programs that are typically associated with the file name extension are displayed.

Information collected, processed, or transmitted
If you choose to use Windows File Association, the file name extension and your computer display language are sent to Microsoft. The rest of the file name is not 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 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
When you try to open a file type without an associated program, you can choose whether to use Windows File Association. 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 7 and Windows Server: Controlling Communication with the Internet article at the Microsoft TechNet website.

Đầu trang

Windows Help

Windows Online Help and Support

What this feature does
Windows Online Help and Support, when turned on, allows you to search for online help content when you're connected to the Internet, giving you the most up-to-date content available.

Information collected, processed, or transmitted
When you use Windows Online Help and Support, your search queries are 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
If you choose the recommended settings during Windows 7 setup, you turn on Windows Online Help and Support. If you do not choose recommended settings you are given the opportunity to select Windows Online Help and Support the first time that you use Windows Help and Support. To change your selection later, click the **Options** menu and click **Settings**, or select **Get online Help** from the toggle menu at the bottom of the Help window.

Help Experience Improvement Program

What this feature does
The Help Experience Improvement Program helps Microsoft identify trends in the way our customers use Help so that we can improve our search results and the relevancy of our content. You may only participate in the Help Experience Improvement Program if you also choose to opt in to use Windows Online Help and Support.

The Help Experience Improvement Program generates a globally unique identifier (GUID) that is stored on your computer and sent to Microsoft with the information described above to uniquely identify your computer. The GUID is a randomly generated number; it does not contain any personal information and is not used to identify you. The GUID is separate from the GUIDs created for Microsoft Error Reporting and the Windows Customer Experience Improvement Program. We use the GUID to distinguish how widespread the issues we receive are and how to prioritize them. For example, the GUID allows Microsoft to distinguish between one customer experiencing an issue one hundred times and one hundred customers experiencing the same issue once.

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
If you choose the recommended settings during Windows 7 setup, you enroll in the Help Experience Improvement Program. You can change your participation settings by clicking the **Options** menu and clicking **Settings**, or selecting **Get online Help** from the toggle menu at the bottom of the Help window. Note that selecting Get online Help from the toggle menu doesn't automatically enroll you in the Help Experience Improvement Program; you must enroll through the settings menu. If you are not enrolled, you will also be given an opportunity to join after submitting feedback.

Đầu trang

ReadyBoost

What this feature does
ReadyBoost can use storage space on some removable media devices, such as USB flash drives and Secure Digital (SD) cards, to improve the responsiveness of your computer. ReadyBoost copies frequently accessed data to the removable media device, where it is accessed by Windows .

Information collected, processed, or transmitted
If ReadyBoost is enabled for a removable media device, ReadyBoost copies encrypted versions of commonly used files and data to the available space on the device.

Use of information
The data stored on your removable media device is used to improve the responsiveness of your computer. No information is sent to Microsoft.

Choice and control

If you add a ReadyBoost-capable media device to your computer, you might be prompted with an option to enable ReadyBoost for the device. You can enable or disable ReadyBoost through the device properties window. Click the **Start** menu, and select **Computer**. In the Computer window, right-click the device, click **Properties**, and then click the **ReadyBoost** tab.

Đầu trang

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. With your permission, the other person can use his or her mouse and keyboard to control your computer and show you how to fix a problem.

Information collected, processed, or transmitted

Windows Remote Assistance creates an encrypted connection between the two computers over the Internet or the local network. When someone uses Windows Remote Assistance to connect to your computer, that person can see your desktop, and any open documents, including any visible private information. In addition, if you allow the other person to control your computer with his or her mouse and keyboard, that person can do things like delete files or change settings. After a connection is made, Windows Remote Assistance will exchange contact information including user name, computer name, and user account picture (the picture displayed on the Start menu). A session log file maintains a record of all Remote Assistance connections.

Use of information

The information is used to establish an encrypted connection and to provide the other person access to your desktop. No information is sent to Microsoft.

Choice and control

Before you allow someone to connect to your computer, close any open programs or documents that you don't want the other person to see. 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. You can disable session logging and contact exchange. For more information about Windows Remote Assistance, see Windows Remote Assistance: frequently asked questions in Windows Help and Support.

Đầu trang

Windows Speech Recognition

What this feature does

Windows Speech Recognition provides speech recognition within Windows and for any programs that choose to use it. Windows Speech Recognition increases its accuracy by learning how you use language, including the sounds and words you like to use.

Information collected, processed, or transmitted

Windows Speech Recognition stores a list of words and their pronunciations on your computer. Words and pronunciations are added to this list using the Speech Dictionary, and by using Windows Speech Recognition to dictate and correct words.

When the Windows Speech Recognition document review feature is enabled, text from Microsoft Office Word documents (with .doc or .docx file name extensions) and e-mail (from e-mail folders other than Deleted Items or Junk Mail) on your computer and on any connected file shares included in your Windows search index locations is collected and stored in one, two, or three-word fragments. One word fragments include only words you have added to custom dictionaries, and two or three word fragments include only words found in standard dictionaries.

All collected information is stored in your personal speech profile on your computer. Speech profiles are stored for each user, and users are not able to access the profiles of other users on your computer. However, administrators can access any profile on your computer. The profile information is not sent to Microsoft unless you choose to send it when prompted by Windows Speech Recognition. You can review the data before it is sent. If you choose to send this data, acoustic adaptation data that was used to adapt to your audio characteristics is also sent.

If you complete a training session, Windows Speech Recognition will ask you whether you wish to send your speech profile data to Microsoft. You can review the data before it is sent. This data might include recordings of your voice while you completed the training session and the other data from your personal speech profile, as described above.

Use of information
Windows Speech Recognition uses words from the speech profile to convert your speech to text. Microsoft uses personal speech profile data to improve our products and services.

Choice and control
You can choose whether to run Windows Speech Recognition. If you run Windows Speech Recognition, document review is on by default. You are given the opportunity to change your document review settings the first time you run Windows Speech recognition. You can change your document review settings or delete personal speech profiles (and most document review data) by going to Speech recognition in Control Panel and clicking **Advanced speech options**. You can also use the Change existing words option in the Speech Dictionary to delete words that you've added to your speech profile. However, deleting your personal speech profile does not delete words added to your personal speech profile through the Speech Dictionary. For more information see Windows Help and Support.

You can control the locations that document review will collect word fragments from by modifying the locations included in your Windows search index. To view or modify what locations are included in your Windows search index, go to Indexing Options in the Control Panel.

At the end of any training session you will be given the choice whether to send your training data and other profile data to Microsoft. You can also send data when Windows Speech Recognition is launched by right-clicking the **Microphone** button, and then clicking **Help improve speech recognition**. In either case, you can view all data files before they are sent, and can choose not to send them.

Đầu trang

Windows Time Service

What this feature does
The Windows Time service automatically synchronizes your computer's time with a time server on a network.

Information collected, processed, or transmitted
The service connects to a time server over the Internet or a local network using the industry standard Network Time Protocol. By default, this service synchronizes with time.windows.com once a week. No information other than standard computer information is sent to the time server.

Use of information
Information is used by the Windows Time service to automatically synchronize the local computer's time.

Choice and control
The Windows Time service is turned on by default. You can turn this feature off or choose your preferred time source by going to Data and Time in Control Panel, choosing the Internet Time tab, and clicking **Change Settings**. Turning off Windows Time Service has no direct effect on programs or other services, but without a reliable time source, the local computer’s clock may become out of synch with other computers on the network or Internet. Programs and services that depend on time may fail or stop working correctly if there is a significant time discrepancy between networked computers.

Đầu trang

Windows Troubleshooting

What this feature does
Windows Troubleshooting allows you to diagnose and fix common problems on your computer. If online settings are enabled, Windows Troubleshooting can search and download troubleshooting packs for specific problems. When Windows Troubleshooting searches for troubleshooting packs, it will send some system information to Microsoft, including information about your computer and the operating system, to determine which troubleshooting packs to offer for your computer. If you attempt

to solve a problem by running a troubleshooting pack, Windows Troubleshooting will preserve the troubleshooting results and actions that were taken to solve the problem. These results can be deleted, or sent to a support professional for additional assistance. If the troubleshooting pack cannot solve the problem, Windows Troubleshooting can help you search for problem solutions in Windows Help and Windows communities online.

Information collected, processed, or transmitted
If online settings are enabled, Windows Troubleshooting will search for and might download a list of troubleshooting packs from Microsoft to help diagnose and fix problems on your computer. If you choose to run a troubleshooting pack that is not on your computer, Microsoft will download the troubleshooting pack to your computer. After running a troubleshooting pack, the results are saved to your computer. These results may contain personally identifiable information, such as a user alias or the name of a device. Windows Troubleshooting can help you search for problem solutions in Windows Help and Windows communities online. Key words associated with the problem will be sent to Microsoft to help find a solution. For example, if your printer is not working correctly and you look for help, the words "printer," "print," and "printing" are sent to Microsoft.

Use of information
Information collected by Microsoft through your use of Windows Troubleshooting is used to help solve problems our users encounter.

Choice and control
If you choose "Recommended settings" during setup, Windows Troubleshooting will search for online troubleshooting packs by default. To change these settings, go to Troubleshooting in Control Panel. Select **Change Settings**, and clear the **Allow users to browse for troubleshooters available from the Windows Online Troubleshooting service** check box. You can also disable online search by clearing the **Get the most up-to-date troubleshooters from the Windows Online Troubleshooting service** check box. To delete troubleshooting results, click **View history**, select a result, and then click **Delete**.

Đầu trang

Điều khoản về Quyền riêng tư của Windows 7