

Windows 10 Privacy Options

Introduction

There are many privacy settings in Windows 10. Some are changeable during the initial Windows setup. During the Windows 10 Upgrade process, you get the opportunity to customise the Privacy settings. You can always change the settings later. Here we explain how to change all the privacy settings after setup.

You might be surprised at the number of privacy intrusions built in to Windows 10!

Recording of keystrokes and voice inputs

Windows 10 and Cortana “get to know you” by recording every keystroke you make, and every request you make to Cortana (the voice-activated assistant).

You can turn this service off, but in doing so you also turn off Cortana.

Start > Settings > Privacy > *Speech, inking, and typing*. To turn this service off, choose *Stop getting to know me*. To turn the service on, click *Get to know me*.

Then go Start > Settings > Privacy > General, then turn off *Send Microsoft info about how I write to help us improve typing and writing in the future*.

Advertising id

Did you know that you have your own personal *advertising id* that Windows lets apps access for targeted advertising? To turn this off,

Start > Settings > Privacy > General, turn off *Let apps use my advertising ID for experience across apps*.

Also set your browser to send “Do Not Track” requests to web sites:

- **Microsoft Edge:** Start Edge, Click the menu (... upper right) > Settings > View advanced settings > turn on *Send Do Not Track requests*
- **Internet Explorer:** Right click Start > Control panel > Internet options > Advanced, scroll down to the Security section, turn on *Send Do Not Track requests to sites you visit in Internet Explorer* > click OK
- **Firefox:** Start Firefox, Menu (3 bars top right) > Options > Privacy > Tick *Tell sites I do not want to be tracked*
- **Chrome:** Start Chrome, Menu (3 bars top right) > Settings > scroll down to *Show advanced settings* > Privacy > Tick *Send a “Do Not Track” request with your browsing traffic*

Location & Geofencing

Windows also tracks your location which apps can use, also geofencing—letting apps know when you enter or exit a particular boundary. If you don’t want apps to know your location:

Start > Settings > Privacy > Location, and turn off all, or particular apps’ ability to use location or geofencing.

Page prediction in Edge browser

Having this on sends your anonymous browsing data to Microsoft and uses extra internet megabytes by predicting what pages you want to browse next. To turn this off:

Start Edge, Click the menu (... upper right) > Settings > View advanced settings > turn off *Use page prediction to speed up browsing, improve reading, and make my overall experience better*.

Improve your Wi-Fi privacy and security

Wi-Fi Sense features should be turned off if you want control over your Wi-Fi connections. Such features as giving your contacts password-free access to your Wi-Fi, accessing paid Wi-Fi services automatically, etc.

Start > Settings > Network & Internet > Wi-Fi > Manage Wi-Fi settings > Turn off *Connect to suggested open hotspots* and *Connect to networks shared by my contacts* and *Enable Wi-Fi services*.

Choose which apps are allowed to use your computer's camera and microphone to capture you dancing and singing and stream the data back to the app owner

Start > Settings > Privacy > Camera , switch off the apps you don't want to use your camera

Start > Settings > Privacy > Microphone , switch off the apps you don't want to use your microphone

While in Privacy settings, also check which apps can access your *Account info, Contacts, Calendar, Email, Messaging, Radios* and *Other devices*—you might be surprised what powerful options are available to these apps!