Bluetooth

# Bluetooth

## Introduction

This guidance helps you use Bluetooth enabled devices and peripheral devices.

[Bluetooth](https://en.wikipedia.org/wiki/Bluetooth) is a very short range WiFi technology. In everyday terms, Bluetooth devices can 'talk to each other' if they are very close, for example in the same room. This makes Bluetooth really good for wireless devices, for example a telephone headset, or a mouse or keyboard.

Bluetooth works by 'pairing' devices. This makes it quick and simple to use. The problem is that Bluetooth, and the pairing process, is not very secure. This means that attackers might get unauthenticated access to devices. As an example, an attacker 'listening' to the Bluetooth connection between a computer and a keyboard could possibly intercept passwords or other sensitive information as the details are typed on the keyboard.

This guidance tells you more about the Ministry of Justice (MoJ) view of Bluetooth, from a security perspective. It also gives you hints and tips on how to use Bluetooth more safely.

The aim is to help you maintain the Confidentiality, Integrity and Availability of MoJ data, applications and services. The results should be that:

* the information you access is not compromised
* you can connect devices using Bluetooth, safely
* you are aware of the problems around Bluetooth, and can take the necessary safety precautions

Note: Remember that there might be local rules that apply regarding the use of Bluetooth devices. A good example is in Prisons, where use of Bluetooth would not be available by default. Ensure that you check with local requirements.

## Accessibility

Some types of Bluetooth devices are not allowed, by default. However, where there is a good reason for requiring a Bluetooth device, such as for Accessibility reasons, then a request for an exception to use the device will be treated sympathetically and permitted wherever possible.

Contact the Cyber Assistance Team by email: [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk)

## Bluetooth devices and risks

Examples of Bluetooth devices, and whether they might be used for business purposes, are as follows:

|  |  |
| --- | --- |
| Bluetooth device | Suitable for MoJ work purposes (Y/N) |
| Keyboards | Y |
| Mouse | Y |
| Telephone headsets | Y |
| Headphones | Y |
| Earbuds | Y |
| Trackpads | N - but exception possible for Accessibility reasons |
| External speakers | Y - but be aware of other people or devices nearby that might be listening |
| Gaming joysticks and controllers | N - but exception possible for Accessibility reasons |
| Laptops | Y - for MoJ-issued devices |
| Hearing aids | Y |
| Watches and Fitness bands | N |
| Smart TVs | N - requires authorisation |
| Storage devices (similar to USB 'thumb' drives) | N |
| Internet-of-things 'Smart speakers' | N |

A Bluetooth device might be at risk from any of the following:

* Eavesdropping
* Unauthorised access
* Message modification
* Denial of service
* Data exfiltration
* Insecure data transmission
* Phishing

An example of a Bluetooth problem is 'bluetooth marketing'. As your walk around with your mobile phone, it is continuously looking for Bluetooth devices and WiFi access points. It does this to help with acurate location tracking. But other devices can also see your mobile phone. These devices might report tracking information about where you were at any time. This guidance will help you understand more about the problem, and suggest things you can do to reduce the risks.

## Best practices for using Bluetooth

Before using a Bluetooth device in a work context, consider the following:

* What is the business case for using the Bluetooth device?
* What data might be or will be access through, or using, the Bluetooth device?
* Does the Bluetooth device have the latest patches and fixes applied - where possible?
* Was the Bluetooth device purchased from a reputable vendor?
* Does the Bluetooth device require a PIN code or similar before connecting?
* Are the Bluetooth devices 'discoverable'?
* Have you connected to any other 'public' Bluetooth devices?
* Are all the devices password protected?
* Might someone be able to see what Bluetooth devices you are using?
* Is the material you are working with OFFICIAL-SENSITIVE or higher?

The best way to ensure your Bluetooth device is as up-to-date as possible is to apply all patches and fixes for all hardware devices as soon as you can.

Bluetooth is a very cheap and simple technology. This means that it is often included in extremely cheap devices; often these use old versions of technology or are not provided with patches and fixes. The best thing is to obtain any Bluetooth devices from reputable vendors, so that it is more likely the device will be supported and maintained correctly.

Many Bluetooth devices try and make connection as easy as possible by enabling 'Direct Connection'. This often means that you only need to 'find' a Bluetooth device on your 'phone or laptop, then click once for a connection to be established. While very easy, this is not safe, because those same direct connections can also happen automatically, 'behind the scenes', without you being aware. If possible, ensure that a Bluetooth connection is allowed only when a PIN or password is supplied. This reduces the risk of 'hidden' Bluetooth connections.

Some Bluetooth devices allow you to choose whether they are 'discoverable'. For example, on Android 'phones, you can go to the Settings -> Connected devices -> Connection preferences -> Bluetooth visibility or similar. The best advice is to change the Bluetooth settings to undiscoverable if you can. Only make the device discoverable when you need to connect to a trusted device.

At regular intervals, check to see what Bluetooth devices are 'known' to your devices. Remove any you don't recognise.

When in public places, make sure you only connect to known devices. Always ensure you are in a secure and safe location such as home, office, or a known isolated place before switching on your Bluetooth.

If someone can see what Bluetooth devices you have, or are using, they might try and use one of their device to intercept or monitor the connection. Try to keep Bluetooth devices out of sight so that no-one knows which ones you might actually be using. Even the bright blue light Bluetooth devices illuminate when they are connected might draw unwanted attention.

Generally speaking, Bluetooth devices do not present extra problems when working with OFFICIAL material. However, the whole point of Bluetooth is to enable and simplify communications, so you need to be extra careful when using Bluetooth devices while working on OFFICIAL-SENSITIVE or higher material.

## Contact details

For any further questions relating to security, contact: [security@digital.justice.gov.uk](mailto:security@digital.justice.gov.uk), or for security advice, contact the Cyber Assistance Team [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk).

## Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [itpolicycontent@digital.justice.gov.uk](mailto:itpolicycontent@digital.justice.gov.uk).