Ministry of Justice

Mobile Device and Remote Working

Security Policy

Contents

Mobile Device and Remote Working Policy

Introduction

This policy gives an overview of mobile devices and remote working security principles and responsibilities within the Ministry of Justice (MoJ). It provides a summary of the MoJ's related policies and guides in relation to mobile devices and remote working.

To help identify formal policy statements, each is prefixed with an identifier of the form: **POL.MOB.xxx**, where **xxx** is a unique ID number.

Audience

This policy is aimed at:

Technical users	These are in-house MoJ Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI, and Knowledge (EPICK) Team.
Service Providers	Any other MoJ business group, agency, contractor, IT supplier, and partner who in any way designs, develops or supplies services, including processing, transmitting,and storing data for, or on behalf of, the MoJ.
General users	All other staff working for the MoJ

“All MoJ users” refers to General users, Technical users, and Service Providers, as defined previously.

Mobile devices

POL.MOB.001: When using mobile devices, special care **shall** be taken to ensure that business information is not compromised. When issuing or using MoJ mobile devices, the following points **shall** be adhered to:

- **POL.MOB.002:** Mobile devices **shall** be registered as an MoJ asset.
- **POL.MOB.003:** Software installation **shall not** be available for general users, except when using an approved MoJ process or tool, such as an MoJ self-service app store.
- **POL.MOB.004:** There **shall** be an ability for remote disabling, erasure or lockout.
- **POL.MOB.005: only** MoJ approved web services and web apps **may** be used.

Use in public places

POL.MOB.006: Care **shall** be taken when using mobile devices in public places, meeting rooms, and other unprotected areas. Protection **shall** be in place to avoid the unauthorised access to, or disclosure of, the information stored and processed by these devices.

The MoJ Cryptography guide offers techniques and information used in the MoJ to support stronger security when using mobile devices.

The MoJ Access Control Guide explains how the MoJ manages access to its IT systems so that users have access **only** to the material they need, in a secure manner.

Theft or loss

POL.MOB.007: Mobile devices **shall** be physically protected against theft, especially when left unattended. Examples include leaving devices unattended in cars and other forms of transport, hotel rooms, conference centres, and meeting places.

Note: Sometimes, it might feel difficult to determine a sensible level of protection. For example, leaving a laptop unattended but in plain sight on the seat of car in a public car park is not very secure. But if the car is parked in an MoJ car park, then the vehicle - and therefore its contents - are probably more secure. The answer is that you should always apply the best possible protection for the assets you are responsible for, at all times. Don't rely on other security mechanisms to provide protection that you neglected to apply.

POL.MOB.008: The MoJ **shall** have, and follow, a clear procedure covering legal, insurance, and security requirements for cases of loss or theft of mobile devices.

Use of private equipment

POL.MOB.009: You **should not** use personal devices for MoJ work purposes.

Exceptions are possible on a case-by-case basis, for example to accommodate Accessibility requirements. To discuss whether you have a case for exemption, contact the Security team in the first instance, *before* using a personal device for work purposes. If an exception is permitted, use of the personal device **shall** be in compliance with MoJ personal device guidance.

Remote working

Remote working refers to all forms of business activity that takes place outside of the office. Remote working is sometimes described as “Working From Anywhere”. Remote working locations include non-traditional work environments or contexts, such as:

- Coffee shops.
- Commuter hubs.
- Co-working spaces.
- Flexible workplace.
- Home offices or workspaces.
- Telecommuting.
- Virtual Work Environments.

POL.MOB.010: The MoJ allows remote working, but the following points **shall** be considered, confirmed, and documented as acceptable during the approval process:

- The existing physical security of the remote working site, taking into account the physical security of the building and the local environment.
- The communications security requirements, taking into account the need for remote access to the MoJ's internal systems, the sensitivity of the information that will be accessed and passed over the communication link, and the sensitivity of the internal systems being accessed.
- Any threat of unauthorised access to information or resources from other persons using the remote working location, for example family or friends.
- The implementation of home networks, and requirements or restrictions on the configuration of wireless network services (wifi).
- Malware protection and firewall requirements.

POL.MOB.011: The guidelines and arrangements for remote working **should** be considered, including:

- The provision of suitable equipment and storage furniture for the remote working activities.

- A definition of the work permitted, the hours of work, the classification of information that may be held, and the internal systems and services that the remote worker is authorised to access.
- The provision of hardware and software support and maintenance.
- The provision of insurance.
- The procedures for information and asset backup, and for ensuring business continuity.
- Audit and security monitoring.
- Limitation or revocation of authority and access rights, and the return of equipment when the remote working activities are terminated.

Enforcement

This policy is enforced by lower level policies, standards, procedures, and guidance.

Non-conformance with this policy could result in disciplinary action taken in accordance with the MoJ's Disciplinary procedures. This could result in penalties up to and including dismissal. If an employee commits a criminal offence, they might also be prosecuted. In such cases, the department always cooperates with the relevant authorities, and provides appropriate evidence.

Incidents

Note: If you work for an agency or ALB, refer to your local incident reporting guidance.

Security Team

- Email: security@justice.gov.uk
- Slack: `#security`

Contact details

For any further questions or advice relating to security, contact: security@justice.gov.uk.

Personal devices

This guidance applies to all staff and contractors who work for the Ministry of Justice (MoJ). It provides advice about using personal devices for work purposes.

Overview

A personal device is any desktop, laptop, tablet, phone, external drive, or similar device that the MoJ does not own.

Note: 'Personal devices' include all personally-owned devices with processing ability or Internet connectivity. This includes all types of assistance, organisational or Internet of Things (IoT) devices. Connected vehicles are a special case discussed in this guidance. In case of any doubt, ask for help about specific examples.

Not everyone has access to an MoJ device for remote use. If you need equipment, you can request it. It can be provided quickly. Contact your Line Manager for details. A request can then be raised through the IT Service Desk.

In unusual circumstances, it might not be possible to organise provision of equipment. In such cases, you **can** request access to an MoJ virtual environment.

Except when connecting to an MoJ virtual environment, or with documented approval in exceptional circumstances as described in this guidance, you **shall not** use a personal device for work purposes.

Avoid connecting peripherals to MoJ devices, unless those peripherals are supplied or approved by the MoJ. Examples of peripheral devices include USB, wireless, or Bluetooth keyboards or mice.

Note: Exemptions are possible for connecting peripherals where accessibility support is required. Contact your Line Manager for documented approval before connecting a peripheral device.

Personal devices **shall not** be charged from the USB ports of an MoJ device.

Note: Specifically: a personal mobile phone **shall not** be charged from the USB ports of an MoJ device.

Guidance

- If you have an MoJ-issued device or virtual environment, you **shall** use that.
- You **shall not** use a personal device to access Google Workspace tools such as Gmail, Docs, Slides, Sheets, Drive, Meet, or Hangouts for work purposes.
- You **shall not** use a personal device to access Office 365 tools such as Outlook email or calendar, Word, Excel, or PowerPoint for work purposes.
    - Wherever possible, an MoJ work device **should** be used to join business Teams calls, either via video or dial in.
    - In cases where staff have not been provided with a work phone or laptop or any other work device which allows them to join or dial into Teams, staff **may** join from their personal devices as a Guest. The chair of the meeting **shall** confirm the identity of each and every person joining their call as a Guest.
- This guidance applies to all tools accessed through a web browser or installed client applications.
- You **shall not** send MoJ information to your personal email account.
- You **shall not** use personal accounts for work purposes.
- You **shall not** store work files or information on a personal device such as a desktop, laptop, tablet or phone.
- You **shall not** store work files or information on a personal storage device or memory stick, such as an external drive, thumb drive, or USB stick.
- Some teams within the MoJ **might** have permission to use personal devices for some tasks. This permission continues, but is being reviewed on an on-going basis. Ensure that you have documented approval recording your permission. Ensure that the permission is no more than 12 months old. To request or refresh permission, ask your Line Manager to seek approval by checking with the Security team.

Note: You are not asked or required to use your own devices for work purposes. Statement **POL.MOB.009** of the mobile device and remote working policy makes clear that you **should not** use personal devices for MoJ work purposes. If you have access to MoJ devices for work purposes, you **shall** use them by default. A special case is that if you do not have an MoJ-issued mobile phone, you **may** use a personal device to receive Multi-factor authentication (MFA) codes or messages which authorise access by MoJ devices to MoJ systems.

Using MoJ tools on personal devices

In accordance with other policy on the use of personal devices, and the use of mobile devices specifically, you **shall not** use personal devices to access MoJ tools, such as MoJ Slack workspaces.

Note: The rest of this section refers to Slack workspaces, but applies equally to other MoJ tools, such as Teams, Trello, Jira, and so on.

You could of course use personal devices to access other (non-MoJ) Slack communities.

The point is that you **should not** use personal devices for MoJ work purposes. Slack workspaces are official MoJ workspaces and **should** only be accessed using MoJ devices.

Personal devices are not allowed to access services or content containing **Official-Sensitive** data. Work devices **shall** be used to access MoJ services such as MoJ Slack communities. If you do not have a work mobile device, and need to access services such as Slack on a mobile device, you **should** request one using Service Now.

Virtual environment

The MoJ provides access to a Virtual Environment to help with exceptional circumstances. This is where suitable provision of a physical device is not possible.

Request a virtual environment through the `Creation of WVD instances` product offering within the Service Catalogue in MoJ Service Now.

Note: A virtual environment does not offer the same capabilities or performance as a physical MoJ-issued device. Using an MoJ-issued device is always preferable.

Connected vehicles

Connected vehicles are effectively Bluetooth-connected storage devices. They are considered personal devices for the purposes of this guidance, regardless of whether they are owned, leased or rented.

Automatic transfer of contact information and calendar events might happen during the pairing process. The resulting transferred data is accessible to any third party who subsequently pairs their mobile device to the vehicle.

Additionally, although such platforms usually offer an option to delete paired profiles, there is currently no confirmation that the data is actually erased to a satisfactory level. Transferred information might not be immediately visible or accessible, but this is not the same as deleting the information from the vehicle.

For these reasons, MoJ devices **shall not** be paired with Bluetooth-enabled vehicles.

Contact details

For any further questions or advice relating to security, contact: security@justice.gov.uk.

Bluetooth

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

Overview

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 Security team by email: security@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
Connected vehicles	N - Connected vehicles are effectively Bluetooth-connected storage devices.

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 you walk around with your mobile phone, it is continuously looking for Bluetooth devices and wifi access points. It does this to help with accurate location tracking. But other devices can also find 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.

Connected vehicles

Connected vehicles are effectively Bluetooth-connected storage devices. They are considered personal devices for the purposes of this guidance, regardless of whether they are owned, leased or rented.

Automatic transfer of contact information and calendar events might happen during the pairing process. The resulting transferred data is accessible to any third party who subsequently pairs their mobile device to the vehicle.

Additionally, although such platforms usually offer an option to delete paired profiles, there is currently no confirmation that the data is actually erased to a satisfactory level. Transferred information might not be immediately visible or accessible, but this is not the same as deleting the information from the vehicle.

For these reasons, MoJ devices **shall not** be paired with Bluetooth-enabled vehicles.

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 find out 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 not discoverable if you can. Only make the device discoverable when you need to connect to a trusted device.

At regular intervals, check to find out 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 find 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 or advice relating to security, contact: security@justice.gov.uk.