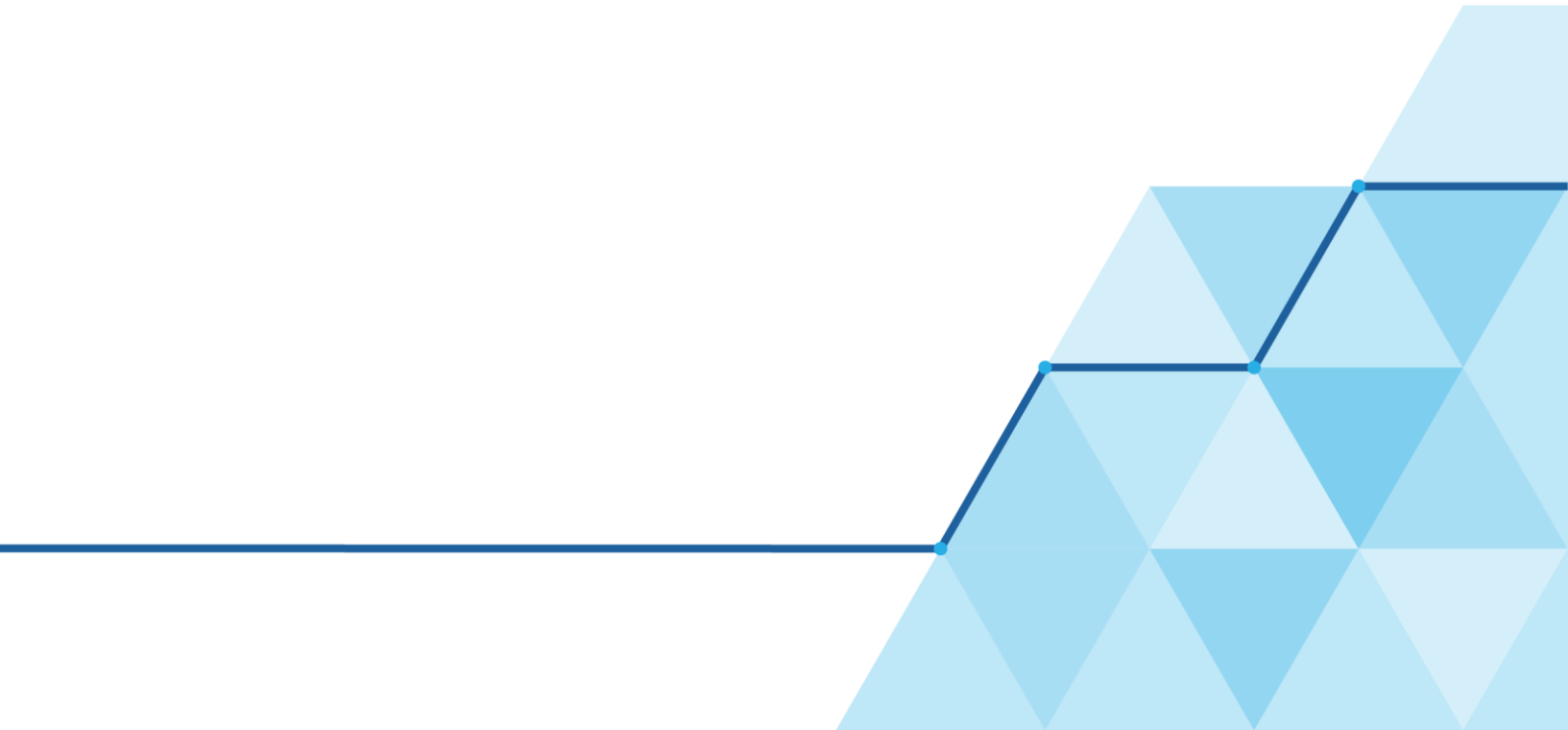
Ministry of Justice

Mobile Device and Remote Working

Security Policy



Contents

Mobile Device and Remote Working Policy 3

Introduction 3
Audience 3
Mobile devices 3
Use in public places 3
Theft or loss 4
Use of private equipment 4
Remote working 4
Enforcement 5
Incidents 5
Contact details 5

Personal device use 5

Guidance 5
Virtual environment 6

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: `POLMOBxxx`, 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 above.

Mobile devices

`POLMOB001`**:** 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:

- `POLMOB002`**:** Mobile devices **SHALL** be registered as an MoJ asset.
- `POLMOB003`**:** 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.
- `POLMOB004`**:** There **SHALL** be an ability for remote disabling, erasure or lockout.
- `POLMOB005`**: ONLY** MoJ approved web services and web apps **MAY** be used.

Use in public places

`POLMOB006`**:** 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

POLMOB007**:** 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.

POLMOB008**:** 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

POLMOB009**:** 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 Cyber Assistance 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.

POLMOB010**:** 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.

POLMOB011**:** 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.

Operational Security Team

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

Contact details

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

Personal device use

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.

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

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, and to raise a request 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.

Note: Except when connecting to an MoJ virtual environment, or with documented approval in exceptional circumstances as described below, you must not use a personal device for work purposes.

Guidance

- If you have an MoJ-issued device or virtual environment, you must use that.
- You must not use a personal device to access Office 365 tools (email, calendar, Word, Excel, Powerpoint, etc.) for work purposes.

- You must not use a personal device to access Google Workspace tools (Gmail, Docs, Slides, Sheets, Drive, Meet, Hangouts, etc.) for work purposes.
- This guidance applies to all tools accessed through a web browser or installed client applications.
- Do not send MoJ information to your personal email account.
- Do not use personal accounts for work purposes.
- Do not store work files or information on a personal device (desktop, laptop, tablet or phone).
- Do not store work files or information on a personal storage device or memory stick (external drive, thumb drive, USB stick, etc.).
- 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 Operational Security Team: security@justice.gov.uk.

Note: You are not asked or required to use your own devices for work purposes. If you have access to MoJ devices for work purposes, you must use them by default.

Virtual environment

The MoJ can enable 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.

© Crown copyright 2021

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.