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: `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 **MUST** be taken to ensure that business information is not compromised. When issuing MoJ mobile devices, the following points **MUST** be adhered to:

- `POLMOB002`**:** Mobile devices **MUST** be registered as an MoJ asset.
- `POLMOB003`**:** Software installation **MUST NOT** be available for general users.
- `POLMOB004`**:** There **MUST** be an ability for remote disabling, erasure or lockout.
- `POLMOB005`**:** There **MUST** be usage of approved web services and web apps **ONLY**.

Use in public places

`POLMOB006`**:** Care **MUST** be taken when using mobile devices in public places, meeting rooms, and other unprotected areas. Protection **MUST** 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 **MUST** 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.

`POLMOB008`**:** The MoJ **MUST** have, and follow, a clear procedure covering legal, insurance, and security requirements for cases of loss or theft of mobile devices.

Protecting sensitive content

`POLMOB009`**:** Devices carrying `SENSITIVE` or important or critical business information **MUST NOT** be left unattended. Where possible, devices should be physically locked away. If this is not possible, approved locks should be used to secure the devices. Contact the Group Security (mojgroupsecurity@justice.gov.uk) or Operational Security (OperationalSecurityTeam@justice.gov.uk) teams for advice and guidance on suitable locking technologies.

Use of private equipment

`POLMOB010`**:** You **MUST 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.

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 includes non-traditional work environments or contexts, such as:

- Commuter hubs.
- Co-working spaces.
- Flexible workplace.
- Telecommuting.
- Virtual Work Environments.

`POLMOB011`**:** The MoJ allows remote working, but the following points **MUST** 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.
- There is no use of personal equipment (equipment that was not issued by the MoJ).
- Any threat of unauthorised access to information or resources from other persons using the accommodation, 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.

`POLMOB012`**:** The guidelines and arrangements to consider include:

- The provision of suitable equipment and storage furniture for the remote working activities. Privately-owned equipment that is not under the control of the MoJ **MUST NOT** be allowed.

- 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 suitable communication equipment, including methods for securing remote access.
- Physical security.
- 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`

Contacts

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