Ministry of Justice

Cyber Security Guidance

General Edition

Cyber and Technical Security Guidance

Summary

This site lists the Ministry of Justice (MoJ) Information Security policies. It contains important guidance on how to keep MoJ information safe and secure.

Policies shown here are listed for technical users and non-technical users (referred to as all users).

Technical users include:

- Technical architects
- DevOps specialists
- IT service managers
- Software developers

The MoJ Technical Guidance covers technical decisions in the MoJ more widely.

Note: This guidance is dated: 5 December 2024.

Change log

A 'change log' is available. It details the most recent changes to this information.

The changes are also available as RSS or Atom feeds.

Searching this content

The MoJ security guidance is searchable in two ways:

1. By searching for the word or phrase on your preferred search engine, and specifying this site:

   ```
   site:https://security-guidance.service.justice.gov.uk/
   ```

   For example, to search for information about passwords, you might use the following search expression:

   ```
   password site:https://security-guidance.service.justice.gov.uk/
   ```
2. By downloading one of the offline versions and using the inbuilt search capability of your offline reader.

Offline content

This offline version of the guidance is available as a PDF file for convenience. However, it is time-limited: it is not valid after 5 January 2025. For the latest, current version of the guidance, refer to the security guidance site.

Security culture

In addition to the obvious security resources such as policies, controls, and software and hardware tools, all organisations need employees, suppliers and other colleagues to behave in a way that helps ensure good security at all times. A simple example is where someone will act in a way that maintains good security, even if they don't know exactly what the formal process is. The extent to which an organisation has good security in indicated by its security culture.

Security culture refers to the set of values, shared by everyone in an organisation, that determines how people are expected to think about and approach security. Getting security culture right helps develop a security conscious workforce, and promotes the desired security behaviours expected from everyone working in or for the organisation.

The MoJ is creating a portfolio of security culture resources to help supplement the formal policy and guidance material. Initial security culture material is available for preview.

Information structure

MoJ policy documents are listed beneath the following headings:

- Information security policies
- Mobile devices and teleworking
- Human resource security
- Asset management
- Access control
- Physical and environmental security
- Operations security
- Communications security
- Information security incident management
- Compliance
- Risk Assessment

The documents are listed in the next section.

Information security policies

Management direction for information security

These are the policies for all users:

- Avoiding too much security
- IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER
- IT Security All Users Policy
- IT Security Policy (Overview)
- Line Manager approval

Mobile devices and teleworking

Mobile device policy

These policies are for all users:

- Mobile Device and Remote Working Policy
- Remote Working

Teleworking

This policy is for all users:

- Personal Devices

Human resource security

Prior to employment

This policy is for all users:

- Minimum User Clearance Levels Guide

Other Guidance

The Government Functional Standard - GovS 007: Security provides the base material for all security guidance in the MoJ.

Glossary

A glossary of some terms used in this guidance is available here.

Acronyms

A more extensive list of acronyms is available here.

Technical Guidance

The MoJ Technical Guidance should be read together with this security-focused guidance.

Feedback

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

Change log for Ministry of Justice (MoJ) Security Guidance

This document summarises what changes were made, and when, to MoJ Security policy and guidance. The most recent changes appear at the beginning of the list.

2023-09-11 17:45 BST Update ITHC details	Updates to information about IT Health Checks.
2023-08-30 17:45 BST Clearance requirements	Added details about minimum user clearance requirements.
2023-08-09 17:35 BST Build tooling updates	Updates to build tooling for security and performance improvements.
2023-07-13 17:00 BST Accessing MoJ IT systems from overseas	Removed topic on accessing MoJ IT systems from overseas.
2023-07-07 16:45 BST Taking equipment overseas	Removed general advice topic on taking equipment overseas.
2023-06-22 17:35 BST Formatting and terminology updates	Minor improvements to formatting, and updates to terminology.
2023-06-05 18:13 BST Updates to incident management policy	Refresh and add extra detail about managing security incidents.
2023-04-29 13:54 BST Add 1Password guidance	Add information about using the 1Password tool.
2023-04-18 17:10 BST Revise content	Updates to personnel and related information.
2023-03-21 17:35 GMT Restructure landing page, and added service owners responsibilities guidance	New material on service owner responsibilities.
2023-02-28 17:35 GMT Corrected policy reference number	Policy number POL.ITAUP.022 in the Acceptable Use Policy was incorrectly listed as number 021.

2022-03-21 10:35 GMT Add guidance on sharing information.	Added extra information on sharing information internally and externally.
2022-03-21 10:22 GMT Add guidance on QR codes.	Added information on QR codes; currently considered low risk.
2022-03-11 15:31 GMT Updates to ransomware information leaflet.	Updates to correct typos and improve style.
2022-03-10 17:01 GMT Updates to LastPass guidance.	More information about when and how LastPass may be used.
2022-03-10 13:09 GMT Various minor corrections.	Fixing broken links and updating references to standards.
2022-03-04 09:16 GMT Updated email security guide.	Clarification that phishing or spoofing of MoJ colleagues, by MoJ colleagues, is not permitted other than with formal approval in advance, justified by a good business case.
2022-02-18 18:35 GMT Added phishing guide.	New topic, providing advice on dealing with phishing threats.
2022-02-16 11:19 GMT Updated security.txt file.	Provided new expiry date for security.txt file.
2022-02-15 12:18 GMT Various minor corrections.	Corrected contact details, fixed an incorrect link, and updated secure disposal information.
2022-02-07 15:49 GMT Updated glossary.	Expanded list of glossary definitions, and explanation of out-of-band-checks.
2022-02-01 11:51 GMT Update to passwords guidance.	A reminder not to share passwords or other account details.
2022-01-25 10:37 GMT Publication of ransomware information leaflet.	Useful leaflet explaining what Ransomware is, and tips on protecting your work and your systems.
2022-01-18 17:06 GMT Updated guidance for hosting platforms.	Updated baseline guidance for AWS and Azure platforms.
2022-01-07 14:36 GMT Contact details for AWS	Updated contact details for Baseline AWS accounts.
2022-01-06 09:36 GMT System lockdown and hardening	Guidance added to prevent outbound connections to random internet systems, unless this is a core part of their design. Firewall rules and other network configuration must prevent this.
2022-01-04 16:27 GMT IT Health Check	Updated guidance with a new section on Cloud platforms.
2022-01-04 16:10 GMT Update Slack channel for privacy team	Provide revised channel details for contact privacy team through Slack IM.
2021-12-23 13:50 GMT Update overseas travel guidance	Updates to information on overseas travel and accessing MoJ IT systems from overseas.
2021-12-21 13:18 GMT Provide seasonal SMS scam advice	Material to help improve awareness and best practices for security.
2021-12-15 15:09 GMT Use DuckDuckGo search engine	Default to using DDG for content search.
2021-12-13 11:44 GMT Security threat level guidance	New security threat Level guidance, and associated procedures.

2021-10-08 09:56 BST Wifi policy	Added policy information about wifi.
2021-10-05 14:28 BST Client certificates	Added notes about obtaining client certificates.
2021-10-01 15:24 BST Connection to public wifi	Clarification about connecting to public wifi spots, such as hotels or coffee shops, or home broadband. Also extra details for remote working securely.
2021-10-01 15:07 BST Personal device attachment	Clarifying the connection of personal peripherals, and the charging of personal devices from USB ports.
2021-09-13 17:21 BST Government Security Standard 007 V2	Updates following the release of V2 of the Gov007 security standard.
2021-09-02 15:16:00 BST Extra guidance on remote working.	Additional best practices for keeping safe and secure when working away from the office.
2021-08-20 14:14:00 BST Update to general apps guidance.	Add Trello guidance, and clarification over Official and Official Sensitive material in apps.
2021-08-18 15:17:00 BST Add change log page.	Created a change log page, and associated RSS and Atom feeds, to describe new or changed content.
2021-08-16 17:04:00 BST Clarification for accessing MoJ IT systems overseas.	Additional information describing the process.
2021-08-16 17:03:00 BST Data Movement Form updated.	Data Movement Form updated.

Getting in contact

Reporting an incident

Ministry of Justice (MoJ) colleagues should visit https://intranet.justice.gov.uk/guidance/security/report-a-security-incident/ on the MoJ Intranet.

Security Team: asking for help

Overview

This document tells you about the Security Team. It explains how to ask for help, outlines how we handle your requests, and describes what happens next.

To ask for help from a security consultant, send an email to: security@justice.gov.uk.

About the team

The Security Team is part of Ministry of Justice (MoJ) Security & Privacy. The MoJ Chief Information Security Officer leads the team.

The team provides help and guidance around cyber security matters, such as:

- Understanding the risks facing your systems and services.
- Designing and implementing effective mitigations for these risks.
- Developing services using security best practices.
- Checking that you or your third party suppliers have enough, and appropriate, cyber security measures in place.
- Applying IT Security policy to specific scenarios.

Asking for help

If you need help dealing with a cyber security task or problem, send an email to: security@justice.gov.uk

Some requests are better handled by other teams. For urgent matters such as incidents, or to get help about physical or personnel security, contact security@justice.gov.uk. For help with data protection, contact DataProtection@justice.gov.uk.

The security team keep an eye open for email requests. Normally, you'll get an acknowledgement or more detailed reply within two working days.

To help us help you, please answer these questions in your email request, as best you can:

1. Who is the work for?
2. Why is it important?
3. What happens if the work is not done (or not done on time)?
4. What is your need (old-style accreditation on an existing contract, guidance or advice, review of proposed approach,...)?
5. What skills or experience does the work need (known or predicted)?
6. When is the next project milestone that needs cyber consultancy input or involvement?

How the team handle requests for help

Each working day, we review all new requests.

We aim to get a reply to you within two working days of us receiving the request. Some large or complex requests might need more information and discussion. These requests take extra time for us to work out the best way to support you.

Some requests might not be appropriate for the team. In such cases, we send a prompt reply, explaining why it would be better to talk with a different team. We'll usually recommend a more appropriate team, and provide contact details for them.

What happens next

If your request is not appropriate for the team, we'll tell you immediately after the initial assessment.

If your request is appropriate for the team, the assigned consultant contacts you directly. They will engage with you to start providing the help you need.

If things go wrong...

If you disagree with our decision about your request, or there is some other problem, contact us again: security@justice.gov.uk.

If you'd prefer a different escalation route, contact ciso@digital.justice.gov.uk.

Security culture

Security culture

This section includes material created or provided by the Ministry of Justice (MoJ) to help improve awareness and best practices for security within the organisation.

Note: The advice in this material cannot guarantee to protect you from problems. The range of security threats is huge, and increasing all the time.

Who is this for?

This material is for anyone who implements, administers, supports, uses or delivers MoJ services.

Christmas SMS delivery scams

Seasonal celebrations are fun, but can also suffer from scams. A common scam involves sending fake parcel delivery text messages. The messages contain fake links. The links capture personal information and bank account details. Bad actors then use these details to steal money from individuals.

Some SMS messages get people to install malware. An example is Flubot, which steals personal and banking details. Flubot also uses your contact lists to send more fake texts.

The best way to avoid SMS scams is to contact parcel delivery companies directly. Go to their website and tracking your parcel there. Never click on a link in a text message.

Contact details

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

Information security policies

Management direction for information security

Avoiding too much security

This guidance applies to developers and system administrators who work for the Ministry of Justice (MoJ).

Is it possible to have too much security? Yes. Providing too much security for things or information that do not need protection is a waste of resources. It undermines the value of the security for things that do need it.

Security by obscurity is one of the weakest approaches for protecting something. It's far better to have a technical control in place to protect the system.

Not all domain names or IP addresses in Government systems are sensitive items

An example is a domain name or IP address. These values do not need to be secret for all systems. Only those that need it. It might be tempting to say that 'all IP addresses are **Official-Sensitive**. This is then used as a reason for an (in)action, such as "I can't email you that network diagram because it contains IP addresses." But the statement has wider consequences. It imposes a set of security requirements for everyone. It imposes them irrespective of the actual secrecy required.

Official-Sensitive is not a different classification to **Official**. It doesn't need special technical controls or procedures. Rather, it's a reminder to look after a piece of information. It's not a controls checklist. Using labels too casually conflicts with the idea of thinking about information and what we're doing with it, and using that to decide how best to secure the information.

Of course, you might need to keep the access details for some systems secure. An example might be where you cannot maintain or patch a legacy system. But these should be exceptional or 'edge' cases.

There are only a small number of situations where you need to protect IP addresses or domain names. It's usually where the context makes the information sensitive in some way. IP addresses can be personally-identifiable information. For example, a system log file might hold the IP address of a client accessing the system. This might reveal a link between an individual and their use of MoJ services. But the IP address of a public sector server or a router should not be personal data.

RECOVER

RECOVER is the core standard to define the minimum of how organisations should recover from an attack once it has been considered closed, and requires:

- identification and testing of contingency mechanisms to ensure the continuance of critical service delivery;
- timely restoration of the service to normal operation (a plan to do so, and testing of that plan);
- from DETECT & RESPOND, immediately implementing controls to ensure the same issue cannot arise in the same way again, ensuring systematic vulnerabilities are proportional remediated.

Contact details

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

IT Security Policy (Overview)

This policy gives an overview of information security principles and responsibilities within the Ministry of Justice (MoJ) and provides a summary of the MoJ's related security policies and guides.

Audience

This policy is aimed at three audiences:

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	Defined as 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.

Within this policy, "all MoJ users" refers to General users, Technical users, and Service Providers as defined previously.

Associated documentation

For further guidance on IT Security, refer to the following policy.

- IT Security All Users Policy: which provides further details of the responsibilities of all MoJ users at the MoJ.

Principles

All MoJ users **shall**:

- Comply with the MoJ's Acceptable Use Policy wherever they work.
- Report all security incidents promptly and in line with MoJ's IT Security Incident Management Policy.
- Make themselves aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other MoJ guidance.
- Be aware of the need for Information Security as an integral part of the day to day business.
- Protect information assets under the control of the organisation.

Further information can be found in the IT Security All Users Policy.

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 MoJ always co-operates 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.

IT Security All Users Policy
Introduction

This policy provides more information on the actions expected of all Ministry of Justice (MoJ) users when using MoJ equipment and infrastructure. It is a sub-page to the IT Security Policy Overview.

Note: In this document, the terms "data" and "information" are used interchangeably.

Audience

This policy is aimed at three audiences:

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	Defined as 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.

Within this policy, "all MoJ users" refers to General users, Technical users, and Service Providers as defined previously.

Approach

The MoJ ensures that IT security controls are designed and implemented to protect MoJ data, IT Assets, and reputation, based around the following requirements:

Confidentiality	Knowing and ensuring that data can only be accessed by those authorised to do so.
Integrity	Knowing and ensuring the accuracy and completeness of data, and that it has not been deliberately or inadvertently modified from a previous version.

Availability	Knowing and ensuring that IT systems and data can always be accessed when required and authorised.

Assets

This policy applies to all premises, physical equipment, software and data owned or managed by the MoJ. This includes IT systems, whether developed by the MoJ or managed by IT service providers. It covers the use of IT equipment and the data processed on those IT systems, irrespective of location. It provides direction and support to preserve the confidentiality, integrity, and availability of MoJ resources.

Security classification

All MoJ Staff are responsible for ensuring data is:

- Classified correctly as detailed in the Information Classification, Handling and Security Guide
- Distributed only in accordance with the statements of this policy and related guides.
- Protected by the appropriate security controls to ensure its confidentiality, integrity and availability.

Physical and personnel security

The Physical Security Policy defines how physical access to assets must be controlled within the MoJ to prevent unauthorised access, use, modification, loss, or damage. All MoJ users must understand that:

- All MoJ IT systems and services must be assessed against environmental risks, for example flood or fire, to maintain the asset's confidentiality, integrity, and availability.
- The MoJ's IT Teams are not directly responsible for the physical security and environment of the MoJ sites.
- Physical security controls and the environment in which the MoJ IT systems operate form part of a system's overall risk landscape. All MoJ users **shall** ensure they adhere to the security controls and requirements set out in this policy.
- Unless otherwise formally agreed by the MoJ, all MoJ users, including agency staff and contractors who have access to MoJ data, require Baseline Personnel Security Standard (BPSS) assessment, as a minimum.
- National Security Vetting should only be applied for where it is necessary, proportionate, and adds real value.
- The MoJ does not have a standing requirement for system administrators or application developers to maintain Security Check (SC) clearance.

Further information on physical and personnel security is available from Security team and CPNI Guidance.

Identity and access control

The MoJ Access Control Guide ensures that information and IT assets can be accessed only by authorised personnel, and that each individual is accountable for their actions.

Email security

The MoJ Email guidance tells you about safe and secure use of email within the MoJ.

Remote working and portable devices

The MoJ has in place Remote Working guidance that sets out the requirements for safely accessing and using the MoJ's systems and applications when working remotely, for example from home, another government office, or while travelling.

Mobile computing is the use of portable equipment such as mobile phone, laptop or tablet, and which supports remote working. Mobile computing equipment provided by the MoJ must be used in line with the Acceptable Use Policy.

Any request to take MoJ IT equipment overseas must follow the guidance provided in the Acceptable Use Policy and the information on accessing IT systems from overseas.

Roles and responsibilities

All MoJ users are responsible for ensuring the confidentiality, integrity, and availability of data within the MoJ. This includes all MoJ data and assets. These responsibilities extend to all assets referenced in this policy.

All MoJ users **shall** comply with the roles and responsibilities outlined in the Information Assurance Framework Process.

Specific roles and responsibilities are described within each sub-page. All MoJ users **shall** comply with these roles and responsibilities, and understand these as being a part of their ultimate responsibility for information security within the MoJ.

For the purpose of this Information Security Policy, the following roles are described. They have specific responsibilities in the implementation and monitoring of different provisions of the policy.

Role	Responsibility	Which includes...
Senior Information Risk Owners (SIROs)	The MoJ SIRO is responsible for the overall MoJ information risk policy and guidance, and ensures that the policy and guidance material continues to provide appropriate risk appetite and a suitable risk framework.	Implementing and managing information risk management in their respective business groups.
		Regularly reviewing the application of policy and guidance to ensure it remains appropriate to their business objectives and risk environment.
		Authorising any exceptions and deviations from the IT Security Policy with consideration of the impact any changes might have to other users.
Delegated Agency SIROs	The delegated agency SIRO is responsible for the information risk policy and guidance as it applies to their systems and personnel, and ensures the agency adheres to the MoJ's risk appetite and risk framework.	In line with the MoJ SIRO, but for Agency systems and personnel.
Information Asset Owners (IAO)	IAOs must be satisfied that all required technical, personnel, physical and procedural security controls are in place and followed. IAOs are responsible for ensuring the management and security of their information asset over the whole asset lifecycle.	Logging and monitoring.
		Reviewing access permissions.
		Understanding and addressing risks associated to their information assets.
		Ensuring secure disposal of information when it is no longer required.
System Owners	System Owners are responsible for managing access control rules for their particular system.	Verifying access rights in order to assist a scheduled review audit of User accounts and permissions.
Contract Owners	Contract Owners are responsible for ensuring contractors adhere to the IT Security Policy set out here and in associated documentation.	Verify that contracts are written to reflect the MoJ's IT Security Policy.

Role	Responsibility	Which includes...
		Ensure contractors comply with the requirements set out by this policy and associated documentation. Being responsible for escalating the risk of non-compliance by a supplier, and seeking guidance on suspected non-compliance with security requirements in a contract. Ensure that the contractor is responsible for any sub-contractors that they employ directly or indirectly, and that the contractor, not the MoJ, is responsible for ensuring that those sub-contractors comply with this policy and associated documentation.

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.

Line Manager approval

This guidance applies to all staff and contractors who work for the Ministry of Justice (MoJ).

Some MoJ IT Policy documents need you to get a review or approval from a Line Manager or other senior person. Do this before taking an action or working in a particular way.

An example is:

- Personal Devices.

This guidance describes what you should do. The guidance contains steps to follow for Line Managers, and their Direct Reports.

Steps to follow (Line Managers)

Note: If at any time you need help about this process, or the applicable MoJ IT Policies, just ask: security@justice.gov.uk.

1. Check that your direct report (DR) has said what they want in their request. The request should identify which MoJ IT Policies apply.
2. Check that the request is valid from a business perspective. If not, deny the request (step 7).
3. Check that Acceptable Use is in the list of applicable policies.
4. Review the requirements or obligations within the MoJ IT Policies that apply to the request.
5. Check that the DR understands and will follow the requirements or obligations. For example, have a discussion with them, or ask them for more information or evidence.
6. If they are able to follow the applicable MoJ IT Policies, send a formal approval to the DR. An email is enough for this.

7. If you don't think they can follow the Policies, or there's a weak business case for the request, refuse it.
8. Keep a copy of your formal reply, in accord with Data Retention requirements.
9. Some MoJ IT Policies need a copy of formal approval for other parties. For example, before your DR travels to some countries on MoJ business, send a copy of your approval to Security team.

Steps to follow (Direct Reports)

Note: If at any time you need help about this process, or the applicable MoJ IT Policies, just ask: security@justice.gov.uk.

1. Check that your business need is valid.
2. Check which MoJ IT Policies apply to your request. Include Acceptable Use in the list of applicable policies.
3. Check that you understand the requirements or obligations within those MoJ IT Policies.
4. Prepare evidence to show that you will follow all the requirements or obligations. Check that you have all the required information.
5. Send a formal approval request to the authorities required by the MoJ IT Policies. Ensure that you include:
   - Your request.
   - The business case.
   - The list of applicable MoJ IT Policies.
   - Evidence that you understand and can follow the requirements or obligations.
6. Be ready to have a more detailed discussion about your request, or to supply more information.
7. If you get formal approval, keep a copy, in accord with Data Retention requirements.
8. If your request is denied, check that you understand the reasons. Use this understanding to tackle your business task again, if appropriate.

Contact details

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

Mobile devices and teleworking

Mobile device policy

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 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.

Current supporting documentation:

- Remote Working
- Security Guidance for Using a Personal Device

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.

Remote Working
Key points

- **Do:** Be professional, and help keep Ministry of Justice (MoJ) information and resources safe and secure at all times.
- **Do:** Think about where you are working, for example - can other people or family access what you are working on? Be thoughtful about information privacy.
- **Do:** Keep MoJ accounts and password information secure.
- **Do:** Take care of your equipment. Devices are more likely to be stolen or lost when working away from the office or home.
- **Do:** Get in touch quickly to report problems or security questions.
- **Do:** Use the VPN if you are handling sensitive MoJ information, or connecting to MoJ systems from a remote location.
- **Do not:** Send work material to personal email accounts.
- **Do not:** Use personal devices or accounts for work purposes - the exception is that a home wifi connection may be used to connect MoJ equipment.
- **Do not:** Leave MoJ equipment unattended.

Overview

The Remote Working Guide gives you advice and guidance on the main security issues that are likely to affect you as a remote worker or a user of mobile computing facilities, (e.g. desktop/laptop computer, smart phones, etc), within the MoJ, including its Agencies and Associated Offices.

It also sets out your individual responsibilities for IT security when working remotely.

Audience

This guide applies to all staff in the MoJ, its Agencies, Associated Offices and Arm's Length Bodies (ALBs), including contractors, agency and casual staff and service providers, who use computing equipment provided by the Department for remote working or mobile computing, or process any departmental information while working remotely or while using MoJ mobile computing equipment.

What is remote working?

Remote working means you are working away from the office. This could be from home, at another MoJ or government office, whilst travelling, at a conference, or in a hotel.

Protecting your workspace and equipment

Remote working is when you work from any non-MoJ location, for example, working at home. It's important to think about confidentiality, integrity and availability aspects as you work. This means protecting equipment, and the area where you work.

- **Do:** Keep MoJ equipment and information safe and secure.
- **Do:** Protect MoJ information from accidental access by unauthorised people.
- **Do:** Lock or log off your device when leaving it unattended. For long periods of non-use, shut down your device.
- **Do:** Ensure that your devices are powered off when you first enter a country when travelling outside the UK.
- **Do:** Keep your workspace clear and tidy. Follow a 'clear desk policy' for information, including paperwork, to ensure MoJ information isn't seen by unauthorised people.
- **Do:** Use MoJ IT equipment for business purposes in preference to your own equipment such as laptops or printers.
- **Do:** Be wary of anyone overlooking or eavesdropping what you are doing. Consider whether you, or the MoJ information, might be Overseen, Overheard, or Overshared.
- **Do:** Protect chargers and other computer accessories, especially MoJ equipment, when travelling. This is to prevent them from being tampered with. Keep them secure and out of sight as much as possible, for example in your hand luggage or on your person.
- **Do:** Ensure that a laptop BitLocker PIN or similar access control is enabled.
- **Do:** Use an MoJ-issued VPN when connecting to Hotel or other public wifi spots.
- **Do not:** Let family or other unauthorised people use MoJ equipment.

- **Do not:** Leave equipment unattended.
- **Do not:** Work on sensitive information in public spaces, or where your equipment can be seen by others.
- **Do not:** Advertise the fact that you work with MoJ materials. However, pre-installed materials such as backgrounds provided as standard with MoJ equipment are acceptable.
- **Do not:** Take part in conference or video calls when you are in public or shared spaces such as cafes or waiting rooms.
- **Do not:** Send your work material to your personal devices or your personal email address.
- **Do not:** Redirect print jobs from MoJ printers to a personal printer.
- **Do not:** Use public 'charging stations' provided at airports, conference venues, hotels, or similar public locations. They might be used to upload malicious software onto your device.
- **Do not:** Connect MoJ equipment to vehicles, using either USB or Bluetooth. These connections can download information from the device or upload malicious software.

Working securely

It's important to consider the security of how you work remotely.

- **Work locations** - as with home working discussed previously, you need to be equally, if not more, vigilant when working in public spaces.
- **Confidentiality** - be aware of others eavesdropping or shoulder surfing, both what you are working on and what you are saying, for example during conference and video calls.
- Keep MoJ **equipment and information**, including printouts and documents, safe and secure.

Even when working remotely, you must still follow the security policies and operating procedures for MoJ systems you access and work with.

Using public wifi or internet, and home broadband

Some locations, such as hotels, coffee shops, or public transport, offer 'public' wifi or internet access.

The public services are usually offered for free. They only need you to agree to some terms of service.

While apparently convenient, these services can have some serious problems:

- They have no security appropriate for protecting MoJ information.
- There is no guarantee about keeping information transmitted through them private or confidential.
- Public services are usually shared. This means that performance can often be very slow and unreliable.

If you need network access, but cannot connect to an MoJ network or home broadband service:

- **Do:** Use an MoJ hotspot. This is usually provided on your MoJ-issued mobile device.

If you need to use a public wifi or internet service, or home broadband, with your MoJ equipment, because you do not have an MoJ hotspot, then:

- **Do:** Connect using an MoJ-issued VPN. Before doing any work, check that the MoJ-issued VPN is working correctly.

Using your own equipment

The main guidance is available here.

- **Do:** Use official MoJ equipment for business purposes.
- **Do not:** Send your work material to your personal devices or your email accounts.

If you are working remotely, or do not have access to MoJ equipment, it might be tempting to use your own equipment, especially printers. Avoid doing this.

Printing

The advice is to avoid printing anything when working remotely, and in particular not to use personal printers.

However, if you really must print MoJ information:

- **Do:** Connect directly to the printer using USB, not wifi.

- **Do:** Consult the information asset owner or line manager before printing the information.
- **Do:** Store any and all printed materials safely and securely until you return to MoJ premises, when they must be disposed of or filed appropriately.
- **Do not:** Print out personal information relating to others.
- **Do not:** Redirect print jobs from an MoJ printer to a personal printer.
- **Do not:** Dispose of unshredded MoJ information in your home rubbish or recycling. Use a cross-cut shredder to destroy printed materials securely, before disposal at non-MoJ locations.

Basically, think before you print.

Privacy

It is important to protect privacy: yours and that of the MoJ. Events like the Covid-19 (Coronavirus) pandemic are often exploited by people wanting to get access to sensitive or valuable information. This often results in an increase in attempts to get access to personal information or MoJ accounts, using phishing and email scams. Be extra vigilant whenever you get an unexpected communication.

Be aware of your working environment when you work with MoJ information. If anyone might access the data, or hear you talk about it as you use it, that could cause privacy problems. Be aware of SMART devices around your remote location, and ensure they are switched off if conducting video or voice communications.

Guidance and suggestions for improving Privacy appear throughout this guide, but it's worthwhile highlighting these points:

- **Do:** Lock your computer, even when unattended for short periods.
- **Do:** Think about whether an unauthorised person, such as a family member, might access the information you are working with.
- **Do not:** Write down passwords. Use a password manager.

Contacts for getting help

In practice, all sorts of things can go wrong from time-to-time. Don't be afraid to report incidents and issues; you will be creating a better and safer work environment.

General enquiries, including theft and loss

Technology Service Desk - including DOM1/Mojo, and Digital & Technology Digital Service Desk. Use one of the following two methods for contacting service desk:

- Tel: 0800 917 5148
- MoJ Service Portal and Live Chat

Note: The previous `itservicedesk@justice.gov.uk` and `servicedesk@digital.justice.gov.uk` email addresses, and the Digital & Technology Digital Service Desk Slack channel (`#digitalservicedesk`), are no longer being monitored.

HMPPS Information & security:

- Email: informationmgmtsecurity@justice.gov.uk
- Tel: 0203 334 0324

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`

Privacy Advice

Data Protection Team

- Email: DataProtection@justice.gov.uk>

- Slack: `#security_privacy_and_live_service_team`
- Intranet: https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/

Cyber Security Advice

Cyber Consultants and Risk Advisors

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

Historic paper files urgently required by ministers, courts, or Public Inquiries

MoJ HQ staff

- Email: Records_Retention_@justice.gov.uk

HMCTS and HMPPS staff

- Email: BranstonRegistryRequests2@justice.gov.uk

JustStore

- Email: KIM@justice.gov.uk

Related information

NCSC Home working: preparing your organisation and staff CPNI Home Working Advice

To access the following link, you'll need to be connected to the HMPPS Intranet.

HMPPS Advice

Teleworking

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.

Related information

Bluetooth on page 87

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.

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.

If the leaver has security clearance, managers should contact the Cluster 2 Security Unit via Security team to advise that the person has resigned and tell them their leaving date or the date on which they will be moving to a different department.

Leavers should read the HR guidance at End or change employment.

Managers must also complete a leaver's checklist as a record of actions.

Downloads

Leavers checklist

A downloadable version of the "End or change of employment" document is available here.

Contact details

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

Asset management

Responsibility for assets

Acceptable use of Information Technology at work

This guidance applies to all staff and contractors who work for the Ministry of Justice (MoJ).

Everyone working at the MoJ has access to MoJ Information Technology (IT) resources. You must use them in an acceptable way. This guidance explains what that means. The definitive list of Acceptable Use Policy statements is here.

Summary

Be sensible when using MoJ IT resources:

- The resources are for you to do MoJ work.
- Protect the resources at all times, to help prevent unacceptable use.
- If the use would cause problems, upset, offence, or embarrassment, it's probably not acceptable.
- Context is important. Security risks can increase when working outside your normal workplace.
- Be aware that your use of resources is monitored. During an investigation into a security incident, IT forensic techniques capture evidence.
- If you're not sure if something is acceptable, ask for help first.
- Above all, if you think there is a problem, report it or ask for help.

The way you use IT is important, because it indicates your approach to work, and can be taken into account when assessing your behaviour and performance.

What is meant by IT?

IT means the devices or services you use for creating, storing, or sharing information. This includes everything from devices (such as laptops, 'phones, mobile Wi-Fi hotspots (MiFi), iPads, tablets, printers, USB "memory sticks") through to online services (citizen-facing online services, staff tools, corporate email).

Acceptable use of MoJ IT

Acceptable use of IT is when you use it to do your work.

IT helps you complete your tasks as efficiently and effectively as possible. Sometimes, you might need account details such as passwords to use the IT. Acceptable use means protecting this kind of information, too.

Personal use of MoJ IT

Limited personal use of MoJ IT is acceptable as long as it does not cause a problem with your work or that of your colleagues. Context is important. For example, doing personal internet banking during your lunch break might be acceptable, but doing the same thing during a work meeting would not.

Personal use of MoJ mobile phones

You might be allocated a mobile phone for use as part of your work. The mobile phone enables you to:

- Make or receive calls.
- Send or receive SMS texts.
- Use Internet services.

This usage must always be for work purposes.

Examples of unacceptable MoJ mobile phone use include:

- Making charitable donations from the mobile phone account.
- Signing up for premium rate text services.
- Calling premium rate telephone services.
- Voting in "reality TV" popularity contests - these usually involve premium rate services.
- Downloading, uploading, or streaming media files that are not work-related, such as music or movies.
- "Tethering" another device to the MoJ mobile phone, and then using the other device for any of the previously mentioned activities.

... as well as any other activities that are not obviously work-related.

All use of MoJ IT resources is monitored and logged. This includes mobile phone usage listed in account bills. It is possible to find out if you used a work-issued mobile phone for unacceptable activities. Unacceptable use is reported to your Line Manager for further appropriate action. Assessing your behaviour and performance takes this kind of activity into account.

Using MoJ IT outside your usual workplace

Some IT resources might be usable away from your usual workplace, such as a laptop. Even outside the office, you must continue to ensure acceptable use of the IT resources.

You should also ask before taking MoJ IT equipment outside the UK.

Avoid using removable media

Removable media like memory sticks are portable and easy-to-use. Unfortunately, this makes them a security risk, so avoid using them. If however they are essential to your work, follow the Use of Removable Media guidance.

Personalisation of equipment

A popular trend is to adorn laptops with stickers. This is acceptable as long as the material does not cause problems such as upset, offence, or embarrassment. The same applies if you customise the desktop environment of your equipment, for example by changing the desktop image.

Contact details

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

Acceptable Use Policy

This document is the Ministry of Justice (MoJ) Acceptable Use Policy. It provides the core set of security principles and expectations on the acceptable use of MoJ IT systems.

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

MoJ Corporate Image

Communications sent from MoJ systems, or products developed using them, such as MoJ branded documents or presentations, **might** damage the public image of the MoJ if they are for purposes not in the interest of the MoJ, or they are abusive, offensive, defamatory, obscene, or indecent, or of such a nature as to bring the MoJ or any its employees into disrepute.

POL.ITAUP.015: All Users **shall** ensure that MoJ systems are not used in an abusive, offensive, defamatory, obscene, or indecent way, or are of such a nature as to bring the MoJ or any its employees into disrepute.

Potential to cause offence and harm

The MoJ has a duty of care to all staff, and to provide a positive working environment. Part of this duty involves ensuring all staff maintain a high standard of behaviour and conduct.

POL.ITAUP.016: MoJ systems **shall not** be used for any activity that causes offence to MoJ employees, customers, suppliers, partners, or visitors, or used in a way that violates the MoJ Code of Conduct.

Personal use

The MoJ permits limited personal use of its IT systems, provided this use does not conflict or interfere with normal business activities. The MoJ monitors the use of its IT systems. Any personal use is subject to monitoring and auditing, and **might** also be retained in backup format, even after deletion from live systems.

The MoJ reserves the right to restrict personal use of its IT systems. The main methods employed are:

- Filtering of Internet and email traffic. All Internet and email traffic is filtered and analysed. Further details are available.
- Policy and procedures. This policy and associated SyOPs set out the restrictions placed on the use of MoJ systems.

POL.ITAUP.017: Users **shall** ensure that any personal use of MoJ systems does not conflict or interfere with normal business activities. Any conflict **shall** be reported to the User's line manager.

POL.ITAUP.018: Users **shall** ensure that any personal use of MoJ systems is consistent with any applicable SyOPs, and with this acceptable use policy.

POL.ITAUP.019: Users **shall** be aware that any personal use of MoJ systems which contravenes any applicable SyOPs, or this acceptable use policy, constitutes a breach of the IT Security Policy and **might** result in disciplinary action.

Maintaining system and data integrity

Users **shall** comply with all applicable operating procedures, and ensure that they do not circumvent any security controls in place. Changes to the configuration of an IT system which affect either the integrity of that system or the integrity of shared data **shall** be undertaken or supervised by an authorised User or system Administrator.

POL.ITAUP.020: All Users **shall** request any changes to systems or equipment through the IT Service Desk.

Electronic messaging and use of the Internet

Due to the risks associated with electronic communications such as email and the Internet, the MoJ controls and monitors usage of MoJ systems in accordance with applicable legal and regulatory requirements.

IT systems are designed to protect the MoJ from Internet-borne attacks, to reduce the risk of MoJ information being leaked or compromised, and to support the MoJ in providing a safe working environment. This is mainly achieved through the filtering and monitoring of all Internet and email traffic.

Also, the use of any high bandwidth services, such as video streaming websites, **might** create network capacity issues, causing poor performance affecting important MoJ services. Therefore, the MoJ restricts access to the Internet, based on job role. Amendments can be made on the submissions of a business case for approval by the MoJ Security team.

The MoJ regards as a disciplinary offence any usage of electric communications, such as email and other methods including instant messaging and the Internet, which breaks the law, contravenes MoJ HR policies, or involves unauthorised access to or handling of material that is deemed to be inappropriate, abusive, offensive, defamatory, obscene, or indecent.

External email and the Internet are, in general, insecure services where it is possible for external entities to intercept, monitor, change, 'spoof', or otherwise interfere with legitimate content. The MoJ deploys a number of security controls to protect its Users from Internet- and email-borne attacks. However, these controls are reliant on Users remaining vigilant, following any applicable SyOPs, and reporting any suspicious behaviour.

POL.ITAUP.021: All Users **shall** use the Internet, email, and other electronic communication systems only in accordance with this acceptable use policy document.

Managing email use

Users are responsible for ensuring that all information is handled in line with the protective marking of that information, in accordance with the Information Classification and Handling Policy.

The MoJ is connected to the Government network, which provides a secure environment for sending or receiving emails between Government departments. This allows Users with an MoJ email account (normally with the suffix '`@justice.gov.uk`') to send **Official** emails with handling caveats such as **Sensitive** to another MoJ or government User, where their email suffix ends in '`gov.uk`'.

POL.ITAUP.022: All Users **shall** ensure that information contained within or attached to an email is handled in accordance with the Information Classification and Handling Policy.

Email is a major source of malware, and a route into the MoJ for criminal organisations. It **might** be used to defraud staff, or to exfiltrate information. All Users **shall** exercise care when handling emails, and report any suspicious activity as an IT security incident.

POL.ITAUP.023: All Users **shall** ensure that they do not:

- Open any attachments to an email where the source is untrusted, unknown, or unsolicited.
- Click on any links within an email, where the source is untrusted, unknown, or unsolicited.

POL.ITAUP.024: Where a User suspects that an email received is from an untrusted, unknown, or unsolicited source, they **shall** report it as an IT security incident.

Connectivity and remote access

Remote access is provided to MoJ systems and services, allowing Users access from offsite and home locations to connect in. The main methods of access are either via a laptop or other mobile device. Normally, remote access is to a protected MoJ IT system. Users **should** be aware of the security controls and procedures of the devices and systems being used, as well as any applicable general physical security considerations. This includes any restriction on the carriage of such devices, as they **might** contain HMG protectively marked data, or HMG cryptographic material.

MoJ security maintains a list of countries where carriage and use of remote access devices is permitted.

Further details can be found in the Remote Working guidance.

POL.ITAUP.025: All Users **shall** be aware of the Remote Working guidance, and **shall** confirm that they have read and understood it before being provided with any remote access devices or equipment, such as an encryption or access control token.

POL.ITAUP.026: Any User wishing to take a remote access device out of the UK **shall** consult the Remote Working guidance before doing so, and the applicable device IT Security Operating Procedures document.

Monitoring of communications

Communications **can** be monitored without notice, and on a continual basis, for a number of reasons. These include compliance with legal obligations, effective maintenance of IT systems, preventing or detecting unauthorised use or criminal activities such as cyber-intrusion, monitoring of service or performance standards, providing evidence of business transactions, and checking adherence to policies, procedures, and contracts.

The MoJ monitors telephone usage, network, email, and Internet traffic data, including sender, receiver, subject, attachments to an email, numbers called, duration of calls, the domain names of websites visited, the duration of visits, and files uploaded or downloaded from the Internet, at a network level.

The MoJ, so far as possible and appropriate, respects User privacy and autonomy whilst they are working, but in accordance with the personal use information, any personal use of MoJ systems is also subject to monitoring. By

carrying out personal activities using MoJ systems, Users are consenting to the MoJ processing any sensitive personal data which **might** be revealed by such monitoring, such as regular visits to a set of websites.

For the purposes of business continuity, it **might** be necessary for the MoJ to access business communications, including within email mailboxes, while a User is absent from work, including for a holiday and because of illness. Access is only granted through submission of a formal request to the IT Service Desk, where approval is required from the relevant line manager. The MoJ Chief Information Security Officer (CISO) and MoJ HR are normally consulted as well, before access is granted.

POL.ITAUP.027: All Users **shall** be aware that their electronic communications are being monitored in accordance with this acceptable use policy.

POL.ITAUP.028: All Users **shall** be aware that business communication such as email mailboxes **might** be accessed if they are absent from work. This access is normally requested through, and authorised by, the User's line manager. The MoJ CISO and MoJ HR are normally consulted as well, before access is granted.

Data protection considerations

Acceptable use considerations apply to the storage of personal data. This storage includes data hosting in 'cloud' environments, or within services or databases hosted or administered outside:

- The UK.
- The European Economic Area (EEA).
- Countries with an Adequacy Decision (an 'Adequacy Decision Country' or ADC).

POL.ITAUP.029: The default position is that MoJ personal data **shall not** be transferred to or through, or stored, in the US or elsewhere outside the UK, EEA, or an ADC, other than in exceptional circumstances.

This position also applies where a supplier uses cloud storage facilities in the UK, EEA, or an ADC, but their employees outside the UK, EEA, or the ADC are able to view the information for activities such as maintenance or trouble-shooting. The effect of this access is equivalent to the personal data being held outside the UK, EEA, or an ADC.

The reason for this position is that even with additional contractual clauses, the MoJ cannot ensure protection of its personal data stored outside the UK, EEA, or an ADC, due to some government surveillance laws.

POL.ITAUP.030: A supplier based in the UK, EEA, or an ADC, and which stores client data in the UK, EEA, or an ADC, **should** be considered first and preferred where possible.

POL.ITAUP.031: If an alternative supplier cannot be sourced, then a Standard Contractual Clause (SCC) and a Transfer Impact Assessment (TIA) **shall** be completed.

These documents are reviewed by the Data Protection Team, after which the transfer **might** be approved. A template for these documents can be requested from DataProtection@justice.gov.uk

POL.ITAUP.032: If the outcome of the assessment does not support the transfer and storage of information outside the UK, EEA, or an ADC, the Information Security and Risk (ISR) Board **shall** review the case, and if appropriate, accept the risks in order for the supplier to be used.

POL.ITAUP.033: This acceptable use policy for MoJ personal data **shall** apply to:

- An existing supplier changing the location of its servers, storage, or services outside the UK, EEA, or an ADC.
- New suppliers.

Data protection acceptable use protocols and standard operating procedures

The Data Protection Team has produced a number of Acceptable Use protocol documents, providing specific data protection guidance.

The documents are available on the MoJ Intranet, or by contacting the Data Protection Team.

The documents are as follows:

- Acceptable Use Protocol Commercial and Contract Management
- Acceptable Use Protocol Subject Access Requests

There are also a number of Standard Operating Procedures (SOP)s, including:

- Personal Data Risk Management
- Data protection impact assessment guidance
- Data sharing agreement assessment

For more information on these protocols and procedures, contact the Data Protection Team.

Contact details

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

Guidance on IT Accounts and Assets for Long Term Leave

Audience and Document Purpose

This document is intended for Ministry of Justice (MoJ) line managers who have a staff member going on any type of long-term secondment, loan, or leave. It provides guidance on how to handle the IT accounts and IT assets (such as desktops, laptops, or mobile phones) of the staff member while they are on leave.

Long term means longer than 2 months.

Types of secondment, loan, or leave where this might apply include:

- Adoption Leave.
- Career Break.
- Loan.
- Maternity Leave.
- Secondment.
- Shared Parental Leave.

For the purpose of this guidance, all of these are examples of "long-term leave".

Guidance Statement
Retaining assets, and access during leave

This guidance applies to assets, defined as being laptops, desktops, or mobile phones.

- A staff member going on any long-term leave may keep their assets while they remain contractually employed by the MoJ, **AND** where the leave is not longer than 12 months in duration.
- Remind your staff member that the Acceptable Usage Policy applies at all times during their leave. The policy can be found here.
- Preparation or return from any type of leave may be accompanied by changes in working patterns. The Remote Working guidance provides useful advice for anyone who may be working remotely for the first time. The policy can be found here.

Note: Devices that are not used for 3 months or more go in to a technical "quarantine", intentionally to render them unusable. Staff members should log in to their devices once per month during leave, to ensure that technical quarantine is not activated. Logging in also helps ensure that system updates are downloaded and applied.

Reviewing access to data and information systems

Before the staff member goes on leave, review their access to data and information systems, to ensure that this meets an ongoing need. This means that:

- If the staff member's role is planned to change on their return to the MoJ, consider removing access now to data and information systems which they will no longer need. If their role is not planned to change on their return, you might consider leaving access "as-is" currently.
- Consider removing access to data or information systems which are **Official-Sensitive**. This is in line with the necessity rigorously to apply the "need to know" principle for **Official-Sensitive** information. Refer to the guidance on classifying information for more detail https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/classifying-information/

It is important to understand that security classification is determined by the level of risk in case of loss or unauthorised access, and not by the type of information.

It is the responsibility of the Data Owner to classify the data.

- Most production data is **Official** information. Within this, some production data might be classified as **Secret** information.
- Most personal data is **Official** information. Within this, some personal data might be classified as **Secret** information if it meets the risk threshold defined.

The following table sets out the definitions for each security classification, as well as whether it is necessary to explicitly "mark" a piece of information with its classification type.

Classification	Definition	Marking
Official	All information related to routine public sector business, operations and services. Almost all personal information falls within the **Official** classification. **Official-Sensitive** is not a separate security classification. It should be used to reinforce the "need to know" principle, beyond the baseline for **Official**.	**Official** data does not need to be marked except where **Sensitive**, and must be marked **Official-Sensitive**.
Secret	Very sensitive information that requires protection against highly sophisticated, well-resourced and determined threat actors, for example serious and organised crime.	Must be marked
Top Secret	Exceptionally sensitive information that directly supports (or threatens) the national security of the UK or its allies and requires extremely high assurance of protection from all threats.	Must be marked

Additional information on how to manage information is described in the Information Asset Management Policy.

Information security classification may change throughout the information lifecycle. It is important to apply appropriate security classifications and continually evaluate them.

The consequences of not classifying information correctly are outlined as follows:

- Applying too high a marking can inhibit business operations, such as collaboration, and lead to unnecessary and expensive protective controls being applied.
- Applying too low a marking may result in inappropriate controls, and may put sensitive assets at greater risk of compromise.
- Incorrect disposal can lead to unauthorised access to information. Disposal of information should be done using approved processes, equipment or service providers.

Official and Official-Sensitive

All of the MoJ's information is, at a minimum, **Official** information. It is very likely that the information you create and use in your MoJ day-to-day job is **Official** information.

Examples include:

- Routine emails you send to your colleagues.

- Deploying, decommissioning and returning data and media.
- Ensuring that any applicable legal, regulatory or contractual obligations are adhered to.

This individual is the Information Asset Owner (IAO). The IAO **shall** ensure that information for which they are responsible for is appropriately handled, and where there is a business requirement to share it with a 3rd party, that it is shared in a safe and secure manner.

Electronic data transfer and storage

Data **shall** be stored only on managed accredited networks, with transfers onto remote access laptops or other mobile devices or media minimised. No sensitive data should be stored on non-networked devices or removable media unless specifically approved by the IAO.

Data in transit

The term "data in transit" covers all electronic moves or transfers of data from one IT system to another, where either the sender or the recipient system is an MoJ IT system. This includes the electronic movement of data using either a system-to-system connection such as CJSE, or removable media such as a USB mass storage device.

Secure network (system-to-system electronic transfer)

The MoJ preference for transferring data is to use a secure accredited government network whether that is a MoJ owner network (e.g. DISC, ONMI, Quantum or MINT) or the Government Secure Intranet (GSi).

As these networks can support data up to and including **Official-Sensitive**, a base level of assurance is provided. However, consideration will need to be given to the following factors to ascertain if any additional security controls are required:

- The amount of data being transferred.
- Frequency.
- Any "need-to-know" considerations.

Any additional controls **shall** be captured on the DMF (refer to the Data Movement Form). Advice should be obtained from the MoJ Security team when required.

USB mass storage device

If using a secure network is not feasible, the next preferred option is to use an encrypted removable media, such as an approved USB mass storage device.

For more information, refer to the Removable Media guidance.

The type of device selected is normally dependant on the sensitivity of the data and the amount of data being transferred. Advice **shall** be sought from the Security team on the best option to use when completing the DMF (refer to the Data Movement Form).

Optical media

The use of optical media (i.e. CD/DVD) is not recommended for data transfer.

Data at rest on MoJ-issued laptops

"Data at rest" is a term used to refer to all data in computer storage. This excludes data that is traversing a network, or temporarily residing in computer memory to be read or updated. The protection of data at rest is achieved by encrypting the hard disk. MoJ-issued laptops use an approved whole disk encryption product. This allows data to be safely stored.

Disposal and decommissioning

Sensitive data **shall not** be kept for longer than is needed. The IAO **shall** check for compliance, including any mandatory retention period.

Physical media containing sensitive data **shall** be disposed of securely, even if that data is encrypted. The reason is that an attacker could potentially make unlimited attempts to crack the encryption used if the media comes into their possession.

Further information on disposal and decommissioning can be found in the Secure Disposal of IT Equipment guidance.

It is important to understand that security classification is determined by the level of risk in case of loss or unauthorised access, and not by the type of information.

It is the responsibility of the Data Owner to classify the data.

- Most production data is **Official** information. Within this, some production data might be classified as **Secret** information.
- Most personal data is **Official** information. Within this, some personal data might be classified as **Secret** information if it meets the risk threshold defined.

The following table summarises the definitions for each security classification, as well as whether it is necessary to explicitly 'mark' or label the information with its classification type.

Classification	Definition	Marking
Official	All information related to routine public sector business, operations and services. Almost all personal information falls within the **Official** classification. **Official-Sensitive** is not a separate security classification. It should be used to reinforce the "need to know" principle, beyond the baseline for **Official**.	**Official** data does not need to be marked except where **Sensitive**, and must be marked **Official-Sensitive**.
Secret	Very sensitive information that requires protection against highly sophisticated, well-resourced and determined threat actors, for example serious and organised crime.	Must be marked
Top Secret	Exceptionally sensitive information that directly supports (or threatens) the national security of the UK or its allies and requires extremely high assurance of protection from all threats.	Must be marked

Additional information on how to manage information is described in the Information Asset Management Policy.

Information security classification may change throughout the information lifecycle. It is important to apply appropriate security classifications and continually evaluate them.

The consequences of not classifying information correctly are outlined as follows:

- Applying too high a marking can inhibit business operations, such as collaboration, and lead to unnecessary and expensive protective controls being applied.
- Applying too low a marking may result in inappropriate controls, and may put sensitive assets at greater risk of compromise.
- Incorrect disposal can lead to unauthorised access to information. Disposal of information should be done using approved processes, equipment or service providers.

Official and Official-Sensitive

All of the MoJ's information is, at a minimum, **Official** information. It is very likely that the information you create and use in your MoJ day-to-day job is **Official** information.

Examples include:

- Routine emails you send to your colleagues.

Example 1

An asset owner creates a report. The report contains potentially private information about individuals. The asset owner decides that the report should be classified as **Official**, with the **Sensitive** handling caveat.

A user wishes to share a copy of the report "as-is" with their team. They cannot remove the handling caveat without prior discussion and agreement from the asset owner.

Example 2

An asset owner creates a report. The report contains potentially private information about individuals. The asset owner decides that the report should be classified as **Official**, with the **Sensitive** handling caveat.

A user wishes to share a subset of the report with their team. In particular, the report is substantially re-worked to remove all the private information. The user becomes the owner of this new asset. They are responsible for this new asset. They can decide that the **Sensitive** handling caveat is not required.

The original report retains its **Official** classification and **Sensitive** handling caveat.

Example 3

An asset owner creates a report. The report contains information about plans to handle a pandemic. The asset owner decides that the report should be classified as **Official**, with the **Sensitive** handling caveat.

A user reviews the report. They realise that the information could potentially compromise the security or prosperity of the country. They decide to increase the classification of the report, and treat it as **Secret**. They discuss this decision with the asset owner, so that the original report is correctly reclassified.

Handling and securing information

The HMG Government Security Classifications Policy is the most comprehensive guide on the security measures necessary for each of the three security classifications, including measures related to the following:

- Personnel (administrative) security.
- Physical security.
- Technical (information security).

The following sections set out the minimum measures you need to consider when handling and securing information within the different levels of classification.

Handling and securing Official and Official-Sensitive information

Type	Measure	Example
PERSONNEL	Make sure all MoJ staff including contractors undergo baseline security clearance checks.	A contractor working with the MoJ Security Team must undergo a baseline background check (i.e. BPSS check) at minimum. Refer to Security Vetting Guidance.
PHYSICAL	Make sure that you lock your screen before you leave your desk. When working in an unsecured area, for example when working remotely, think about whether unauthorised people might be able to eavesdrop on your conversations, or look over your shoulder at your screen.	

Contact details

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

Secure disposal of IT equipment

The Ministry of Justice (MoJ) and its Executive Agencies and Arms Length Bodies use a wide variety of equipment, both physical and virtual. These resources are procured and managed though MoJ suppliers, who are normally responsible for the secure disposal of the resources when no longer used.

However, there are also other physical and virtual resources across the MoJ estate which might have been procured and managed locally. It is crucial that they are disposed of in a secure manner, to prevent data being leaked.

Note: When disposing of **Secret** or **Top Secret** equipment, materials, or resources, you **shall** contact security: security@justice.gov.uk

Contact details

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

Secure disposal of IT - physical and on-premise

This document is the Ministry of Justice (MoJ) guidance covering disposal of physical and on-premise media and data. It is intended to ensure that the confidentiality and integrity of MoJ data is maintained when physical hardware is decommissioned.

Physical Media and Associated Data

The MoJ and its Executive Agencies and Arms Length Bodies use a wide variety of equipment, including photocopiers and printers, data centre hard and tape drives, desktop computers, laptops, USB memory sticks, and generic mobile devices. Some equipment might be the responsibility of a supplier to decommission and dispose of it safely and securely. Check asset tags or similar identifiers to determine and validate responsibility.

However, other devices across the MoJ estate might have been procured and managed locally. They **shall** be disposed of securely, to prevent MoJ information from being “leaked”.

Approved organisations

For help to arrange secure disposal by an approved organisation, contact IT Service Desk (0800 917 5148).

NCSC and CPNI on Secure Disposal

The National Cyber Security Centre (NCSC) and Centre for the Protection of National Infrastructure (CPNI) give critical guidance on the secure sanitisation of storage media here and here, respectively, specifically regarding disposal and destruction of media, and the data contained within it.

The situations when sanitising data is required are:

- Re-use.
- Repair.
- Disposal; sanitising unwanted media and its associated data whilst it is controlled by the MoJ and before it is passed outside the MoJ.
- Destruction; destroying the media, and hence data it contains, onsite or offsite.

Determining data deletion and destruction methods

To determine the data disposal and the media's destruction method, based on the type of equipment and its security classification, use the following table.

The table contains two columns, called “Data deletion method” and “Destruction method”, which are defined as:

Data deletion method	Covers assets if they remain within the MoJ, and have not reached end of life. For example, the device can be re-used or reallocated to a different user, or repurposed for a different function.

There are different controls regarding how the various levels of classified information are secured. Refer to the Information classification, handling and security guide for more information.

Taking documents and files out of the office

Occasionally, you might need to take MoJ information outside MoJ premises. Examples might be when you are working from home, or moving between MoJ buildings. At such times, it is likely that you'll be carrying valuable information within documents, paper files and personal notebooks.

POL.PPR.007: Always check first whether it is really necessary to take documents out of the office. If it is essential to do so, you **shall** get permission from your line management, especially if the information includes:

- Personal information, including anything that relates to an identifiable individual or individuals, such as MoJ staff, stakeholders, partners, or customers.
- Material marked **Official-Sensitive**.

POL.PPR.008: You **shall** get permission from a head of division, or from a member of the Senior Civil Service (SCS) if the information is marked at a level higher than **Official-Sensitive**. Removal or relocation of information marked at a level higher than **Official-Sensitive shall** be noted and recorded on a register, and a record kept of when the material is logged back in.

POL.PPR.009: If you are carrying papers out of the office, you **shall** protect them against accidental loss such as an accident or distraction, causing you to drop or misplace them.

POL.PPR.010: Ideally, carry papers in an unmarked case. For papers marked **Official-Sensitive** or higher, or when using public transport, you **shall** use a lockable case.

POL.PPR.011: For short journeys, such as on foot, and where you are not stopping or using public transport, it is acceptable to carry **Official** papers in a plain envelope, marked only with your name and office address.

POL.PPR.012: If carrying papers to a meeting at a different location, you **shall not** allow sensitive details to be visible. The reason is that they could be photographed by a journalist.

POL.PPR.012.001: Papers **should** be stapled together or otherwise secured in a package. This is to limit dispersal if the carrying case or envelope becomes damaged or opened.

POL.PPR.013: Cases or envelopes **should** have the minimum details necessary on the outside to assure safe return of the item, if lost, without having to be opened to reveal the contents.

POL.PPR.014: Documents **shall not** be left unattended in public places or in an unattended car. Care **should** be taken if you are reading protectively marked information in public places where you might be overlooked, such as a train, or where it might be difficult to retrieve a document if you lost hold of it, for example if you dropped it, or it was blown away.

If you are taking papers home, ensure that they are not readily accessible to other members of your household. Take precautions to minimise their loss. If the papers would normally be locked away in the office, try to do the same at home.

Sending documents

Options for sending documents are covered in the Sending Information guidance note.

Disposing of paper information

MoJ offices have bins or bags that are specifically intended for secure waste disposal of documents or files, including:

- Personal information that relates to an identifiable individual or individuals.
- Sensitive information that **should not** be disclosed.
- Any material bearing a visible classification marking.

POL.PPR.015: You **should** read and follow the secure waste disposal guidance on the MoJ Intranet before disposing of any document or files.

POL.PPR.016: Before disposing of information, you **should** check whether it should be retained on a file, and whether it is covered by a 'retention schedule'. The Records and Retention team can advise on this.

Sharing passwords

To share a password, create a Vault.

You **should** make sure the credentials you're sharing are only available to the people who need to access them for MoJ work. It is your responsibility to remove items or people from vaults when access to the credential(s) is no longer required.

You **shall not** share your 1Password main password with anyone, even your line manager or MoJ security.

Using it overseas

Taking a device (such as personal smartphone) that has MoJ 1Password installed counts as travelling overseas with MoJ information.

The MoJ has existing policies on travelling abroad on the MoJ intranet, which require various approvals before travel.

It may be simpler to 'log out' of the 1Password applications or enable Travel Mode to remove vaults from your devices. These can be reinstated when you return to the UK.

Keeping 1Password update to date

Like all software, it is important to keep the software up to date (sometimes known as 'patching'). 1Password software generally self-updates to the latest version by itself, however make sure you approve or apply any updates if 1Password asks you to.

Need help?

If you need help *installing* 1Password contact the relevant MoJ IT Service Desk.

If you need help using 1Password such as getting access to vaults or resetting your primary password as you have forgotten it, contact Operations Engineering Team through their Slack Channel, `#Ask-Operations-Engineering`, or email Operations Engineerings.

Physical and environmental security

Equipment

Clear screen and desk

There are many helpful policies and best practices that improve Ministry of Justice (MoJ) safety and security.

Note: In addition to this advice in this document, you should review and follow the guidance in the remote working guidance, for example thinking before you print.

Clear screen

Users **shall** comply with the following:

- MoJ equipment **shall not** be left logged on when unattended. Users **shall** ensure that password-protected screensavers are activated when any equipment is left unattended.
- Computer screens **shall** be angled away from the view of unauthorised persons.
- Computer security locks **shall** be set to activate when there is no activity for a short pre-determined period of time. This timeout **should** be set to 5 minutes, by default. The screen lock **can** be manually activated when required.
- Computer security locks **shall** require passwords to be re-entered to reactivate the computer.
- Desktops and laptops **should** be shutdown if you expect to be away from them for more than half an hour.
- Users **shall** log off or lock their computers when they leave the room.

A best practice is to keep your screen 'desk top' tidy:

As a result, it might be preferable to use a new machine, rather than repurposing a reassigned device. The decision depends on the expected use of the reassigned device.

The LM is responsible for ensuring a review of the equipment. This is to ensure that sensitive data **shall not** be lost by erasing the contents of the device. This task **can** be delegated to the team member most familiar with the data. The LM remains responsible. Any sensitive data identified **shall** be copied and relocated to a secure location. This can be the MoJ Teams facility or to Sharepoint. This **shall** happen before the device is made ready for reuse or destroyed.

Any IT equipment which is no longer needed, or has reached its "end of life" **shall** have its data securely deleted and confirmed to be unreadable and unrecoverable before destruction, redistribution, or reuse of the equipment.

Equipment Reassignment

Equipment **can not** be passed from one user to another without being formally reassigned.

Equipment **shall** be completely "cleaned" to an "as-new" state before it is reused or reassigned. This means that all storage media in the device **shall** be fully erased. A sufficiently secure method for "wiping" equipment **shall** be used. Deleting visible files, emptying files from the "Recycle Bin" of a computer, or reformatting a device are not considered sufficiently secure methods for wiping equipment. The reason is that data recovery software might be used by a new owner to "undelete" files or "unformat" a device.

To erase data securely, use appropriate "data-shredding" tools for the media being erased. Typically, these tools do not simply delete data, they overwrite it multiple times. The overwriting erases all traces of the data, making it almost impossible for any retrieval. Another option is to re-encrypt the device using a different password, then delete the data to free up space.

Equipment reassignment **shall** be recorded by the LM in the appropriate asset register.

Equipment that cannot be reused

If IT assets are no longer needed by the MoJ, and cannot be securely wiped, then the equipment **might** need to be destroyed physically. More information can be found at Secure disposal of IT equipment

Regrettably, for security reasons, redundant IT equipment **should not** be donated to charities, schools, or similar organisations.

Leased equipment

Managers **should** ensure that any equipment that is leased has a data destruction clause written into the contract. Under such an arrangement, the supplier **shall** ensure that data is wiped when it is returned.

Contact details

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

Laptops

The guidance applies to all Ministry of Justice (MoJ) staff.

Related information

Lost devices or other IT security incidents on page 124

Storing data on laptops

If you need to store data on your computer you should always remember to move it into:

1. Your local Electronic Document and Record Management (EDRM) system.
2. An MoJ shared drive.
3. Your MoJ-provided 'home' drive.

Do this as soon as you can next connect to the MoJ network.

Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI, and Knowledge (EPICK) Team.

2. **Service Providers**: defined as any other MoJ business group, agency, contractor, IT supplier, or partner who in any way designs, develops, or supplies services (including processing, transmitting, storing data) for, or on behalf of, the MoJ.
3. **General users**: all other staff working for the MoJ.

The phrase "all MoJ users" refers to General users, Technical users, and Service Providers as defined previously.

Transfer Considerations

Anyone handling personal or sensitive data must seek consent from their line manager to authorise data transfer.

Before any data transfers are requested, consider the following:

- Is it strictly necessary for the effective running of the MoJ, and the care of the people it serves, that the data (regardless of whether the data is sensitive or not) is transferred?
- What is the nature of the information, its sensitivity, confidentiality, or possible value?
- What is the size of the data being transferred?
- What damage or distress might be caused to individuals as a result of any loss or unmanaged sharing during transfer?
- What implications would any loss or unmanaged sharing have for the MoJ?
- What information is actually necessary for the identified purpose? For example, is the intention to send an entire document or spreadsheet, when only one section, or specific spreadsheet columns, are required?
- Has the identity and authorisation of the information recipient been established?

Any transfer technique used **shall**:

- Encrypt the data over the network (in transit), using sufficient and appropriate encryption (currently TLS 1.2 or greater).
- Require strong authentication to ensure that both the sender and recipient are who they claim to be.

These considerations apply when transmitting any data over a wireless communication network (for example wifi), or when the data will or might pass through an untrusted network.

If the MoJ is the controller of the data being transferred, the security storage requirements at the destination **shall** be considered to ensure that they comply fully with the relevant regulation, such as PCI DSS or GDPR.

If it's not clear who the data controller is, ask the Data Protection Team for help.

When dealing with third parties, consider whether any data sharing agreements or contracts are in place that apply to the transfer of that data. Check whether there are any stipulations in place regarding the method of transfer that can or should be used.

If personal data is being transferred to a third party, then the privacy team **shall** be informed, to decide if a Data Protection Impact Assessment is required.

Data Transfer

Normally, files **should not** be transferred by email. Normally, files **should** be transferred by secure network links using appropriate protocols such as `https`, `ssh`, or `sftp`. For large files, such as those over 5MB, transfer using a secure protocol is a practical necessity, as many recipients will not accept emails with attachments greater than 5MB.

Data Transfer by Secure link

The MoJ's preferred method of data sharing is to use Microsoft Teams via Sharepoint. Teams has been authorised to hold **Official-Sensitive** information. It is configured to provide greater granular protection through tools such as Azure Information Protection (AIP). Where possible, data **should** be transferred using Teams.

Due to the diverse nature of the MoJ's architecture, using Teams might not always be possible. Those in the MoJ Digital and Technology team who do not have access to Microsoft Teams **may** use Google Workspace to transfer data.

- 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.

Current supporting documentation:

- Remote Working
- Security Guidance for Using a Personal Device

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.

- Don't open unexpected attachments or click on strange links in emails, even if the email appears to be from someone you know. Check the style and content; if it isn't consistent with previous emails, it could be a scam.
- Do not reveal personal or other sensitive information in response to automatic email requests.
- Avoid sharing your business email address on the internet. These might be collected and used by automatic 'harvesting' software programs.
- Never use your MoJ email address to register for non-work related sites.

If you think you've received a scam email, or a virus, report it immediately. Do not click on any link or forward it to anyone. Only delete it from your inbox when you have been told to do so.

Further reading from the NCSC

Email security and anti-spoofing

Other email problems
Auto-forward

Auto-forwarding is where you get your email system to send emails automatically to another account. This might seem very useful, especially if for some reason you can't access your normal business email account, for example while you are away on holiday.

But auto-forwarding is very risky.

You can't be certain that the forwarded emails are safe to send to the new account. For example, the new account might have weaker technical security, making it easier for a hacker to break in and read your email.

You might also be auto-forwarding emails sent to you from outside the MoJ; perhaps from another government department or commercial organisation.

When an email is sent to you, you are responsible for ensuring that everything in the email is handled correctly. This means looking after it to the standard required for that information. You mustn't send that information to another email address, where the required security standards might not be met.

Never use auto-forwarding to forward emails from your MoJ business email address to another non-MoJ email address. In particular, never forward email from your MoJ business email address to a personal email address.

Note: An external email service is any service that is outside the `gov.uk` domain.

There might be occasions when you have a genuine business need to auto-forward email to another email account, where the new address has the same or higher security standards. An example is forwarding from an MoJ business email address to another MoJ business email address. If you have business need for this, ask for help.

Chain letters

These are letters sent to several people who are asked to send copies to several others. They sometimes threaten that bad things will happen if the letter is not forwarded. Chain letters are a hoax.

Chain letters usually do not have the name and contact information of the original sender so it is impossible to check on their authenticity.

Legitimate warnings and solicitations will always have complete contact information from the person sending the message.

Newer chain letters may have a name and contact information but that person either does not exist or is not responsible for the hoax message.

Warnings without the name of the person sending the original notice, or warnings with names, addresses and phone numbers that do not actually exist, are probably hoaxes.

Don't circulate warnings yourself; real warnings about viruses and other network problems are issued for everyone by MoJ technical services.

Note: When in doubt, don't send it out.

- Do not go to any external site if directed from an unsolicited call.
- Never give any information about your computer to the caller.
- Check if the call is genuine with your IT Service Desk. Report the call as a security incident if it is not. Use a different phone from that used to take the original call.

Hoaxes

Hoax letters are designed to trick you into believing, or accepting as genuine, something false and often preposterous: the messages they contain are usually untrue.

Hoax messages try to get you to pass them on to everyone you know using several different methods of social engineering. Most of the hoax messages play on your need to help other people. Who wouldn't want to warn there friends about some terrible virus that is destroying people's systems? Or help this poor little girl who is about to die from cancer?.

Chain letters and hoax messages have the same purpose but use a slightly different method of coercing you into passing them on. Chain letters, like their printed ancestors, generally offer luck or money if you send them on (scams). They play on your fear of bad luck and the knowledge that it is easy for you to send them on. Scams play on people's greed and are illegal no matter what they say in the letter.

The risk and cost of hoaxes

The cost and risk associated with hoaxes may not seem to be that high. If, however, you consider the cost of everyone within the MoJ receiving one hoax message, spending two minutes reading it and another two minutes forwarding it on or discarding it, the cost can be significant.

Handling these messages may also make our mail servers slow down to a crawl or crash.

Spammers (bulk mailers of unsolicited mail) may harvest email addresses from hoaxes and chain letters. Many of these letters contain hundreds of legitimate addresses, which is what the spammers want. There are also rumours that spammers are deliberately starting hoaxes and chain letters to gather email addresses.

How to recognise a hoax

A request to "send this to everyone you know" (or some variant) should raise a red flag. The warning is probably a hoax. It's unlikely a real warning message from a credible source will tell you to send it to everyone you know.

If the warning uses technical language, most people, including technologically savvy individuals, tend to believe the warning is real.

There may be credibility by association. If the janitor at a large technological organisation sends a warning to someone outside of that organisation, people on the outside tend to believe the warning because the company should know about those things. Even though the person sending the warning may not have a clue what he is talking about, the prestige of the company backs the warning, making it appear real.

These make it very difficult to be certain a warning is a hoax. Check if the claims are real, and if the person sending out the warning is a real person. Ask yourself if they are someone who would know what they are talking about.

Type of hoaxes

Scam chains

Mail messages that appear to be from a legitimate company but that are scams and cons, for example Advance fee scams.

Giveaways

Stories about giveaways by large companies. If you only send this on, some big company will send you a lot of money, clothes, a free vacation, etc., etc. You would have to wait forever for any of these to pay off.

Malicious warnings (virus hoaxes)

These are warnings about Trojans, viruses, and other malicious code, that have no basis in fact.

Virus hoaxes have flooded the internet with thousands of viruses worldwide. Paranoia in the internet community fuels such hoaxes. An example of this is the "Good Times" virus hoax, which started in 1994 and is still circulating the

Many tools lets you export your data. You can then store it on an appropriate MoJ system. Sometimes it's easier to copy and paste text into a new document. Make sure that only the correct people have access to the information. This is important after staff or organisational changes, for example.

For more guidance, read the Information Management section on the Intranet. There is also help on responding to requests for information.

Acceptable Use

You must use communications tools for business purposes in an acceptable way.

Be sensible when using communications tools for MoJ business purposes:

- Be extra careful with sensitive and personal information in tools.
- Try to avoid using the same tool for business and personal use - you can get confused who you're talking with.
- If the message you're about to send might cause problems, upset, offence, or embarrassment, it's not acceptable.
- Context is important - a message you might think is funny could be upsetting to someone else.
- If something goes wrong, report it.

The bottom line is:

> If there is doubt, there is no doubt - ask for help!

Approved tools

Tool name	**Tool type**	**Conditions/ constraints on use**	**Accessing /installing tool**	**Audience**
Apple Facetime	Communication tool: Video	Avoid personal or sensitive data	Smartphone App	Internal/ External
Apple iMessage	Text messaging	Avoid personal or sensitive data	Smartphone App	Internal/ External
Google Meet (was Google Hangouts)	Communication tool: Video and/or voice	MoJ use approved for **Official** and **Official-Sensitive**	IT Service Desk controlled Mac - Self service, Web browser.	Internal/ External
Microsoft Teams	Communication and collaboration tool: Video and/or voice	MoJ use approved for **Official** and **Official-Sensitive**	Dom1 Software centre, IT Service Desk controlled Mac - Self service, Web browser.	Internal/ External
Miro	Collaboration tool: Whiteboarding	Avoid personal or sensitive data	Web browser.	Internal/ External
Skype for Business	Communication tool: Video and/or voice	MoJ use approved for **Official** and **Official-Sensitive**	Dom1 Software centre, IT Service Desk controlled Mac - Self service, Web browser.	Internal/ External
Slack	Text messaging, Voice/ Video calls, etc.	Avoid personal or sensitive data	IT Service Desk controlled Mac - Self service, Web browser.	Internal/ External
Slido	Q&A tool during presentations	Avoid personal or sensitive data	Web browser.	Internal

Tool name	Tool type	Conditions/ constraints on use	Accessing /installing tool	Audience
Trello	Project management tool, 'Kanban' cards	Avoid personal or sensitive data. An enterprise-wide MoJ licence is available. Ensure you create Trello boards in the MoJ workspace. Do not use a personal Trello account.	Web browser based use. Log in using your MoJ single sign-on account, for example a Digital & Technology Google account, or a Microsoft Office 365 account.	Internal
Twitter	Text Messaging, Video transmission	Approved for MoJ Corporate account. Using a personal account to comment on work related issues is encouraged, as long as you follow the Civil Service Code of Conduct.	Web browser, Windows 10 App, Smartphone App.	Internal/ External
WhatsApp	Text messaging, Voice/ Video calls	Avoid personal or sensitive data	Dedicated app on device, also web browser.	Internal/ External
Yammer	Text messaging	Avoid personal or sensitive data	Dedicated app on device	Internal
YouTube	Video sharing tool: Video, streaming and chat	Avoid personal or sensitive data	Web browser based use.	Internal/ External
Zoom	Communication tool: Video, voice and chat	Avoid personal or sensitive data	Web browser based use, or dedicated and installed app by approval	External meetings. For Internal meetings, use Microsoft Teams.

Password managers

MoJ guidance encourages the use of password managers where possible. To establish what options are available for an MoJ-issued device, check the official MoJ software and application installation tool provided with the device, to see whether it includes a facility to install optional software and whether a password manager is among the options.

Tools for sharing information internally and externally

For secure sharing and transfer of materials within MoJ bodies or external organisations including other government departments, the MoJ installation of Microsoft Teams is approved for use with data up to and including **Official-Sensitive**.

For secure sharing and transfer of materials with external organisations that cannot use Teams, the Criminal Justice Secure Exchange (CJSE) and Criminal Justice Secure Messaging (CJSM) tools are the preferred solution for data up to and including **Official-Sensitive**.

For secure sharing and transfer of materials with external organisations where the use of Teams, CJSE, or CJSM is not practicable, the following tools are approved for data up to and including **Official-Sensitive**:

- Egress (NCSC certified)
- Galaxkey (NCSC certified)

For use within MoJ bodies, these products may only be installed on MoJ-issued devices. For advice on installation and configuration of these products, consult the team responsible for the supply and configuration of your devices.

For secure sharing and transfer of materials with other government bodies, where the use of Teams, CJSE, CJSM, Egress, or Galaxkey is not possible, the use of official MoJ email systems is approved for data up to and including **Official-Sensitive**.

Always follow the guidance in the Data Handling and Information Sharing Guide when making such transfers. This applies particularly with regard to the sharing of data classified higher than **Official**.

If you need clarification or further assistance in selecting the appropriate tool, ask for help.

Proctoring software

You **shall not** install proctoring software onto MoJ equipment.

Some certification or examination organisations enable people to take assessments remotely. They do this by having 'supervision' software installed on the user's computer. This software is often referred to as 'proctoring software'. The tools make sure that the assessment is as fair as possible, by installing a variety of controls. For example, the software can take control of the camera and microphone of the device it is installed on.

The problem is that the controls give the proctoring software extensive access to the computer. This means that the tools could inspect information or other applications on the computer. In effect, the proctoring software might have uncontrolled access to MoJ information or materials on the computer. This is not acceptable.

If you need to use proctoring software, your options are:

- Install the proctoring software on a personal device.
- Contact the assessment organisation asking for alternative options.

NHS Track and Trace

The official NHS Covid-19 app was designed by the NHS. Both NCSC and Cabinet Office have been involved in the security of the system. The app provides contact tracing, local area alerts and venue check-in. It enables you to protect yourself and your loved ones. Installation is optional, but recommended.

After installing the app, you'll receive an alert if you have been in close contact with other people who have tested positive for coronavirus. You can then take action to avoid passing the virus on, for example by self-isolating.

From a security perspective, it is safe for you to use the app on your personal or MoJ issued devices. There are no extra risks for colleagues with security clearance, such as SC and DV.

If you wish to install the app, start at the NHS site.

Note: The NHS app may not work on some older MoJ devices. Installation might not be possible, for example on MoJo smartphones.

You might have both a personal and an MoJ issued device. Think about which device makes most sense to use with the app. It's best to install on the device that you carry with you and use most of the time. You could install on all your devices if you prefer.

To reduce the likelihood of false alerts on the app, turn off the app's Bluetooth mode. Do this when:

- You are working in environments with protective Covid measures in-place, for example plexiglass separators.
- You need to leave your personal or work device in a locker, for example during a sports activity or to work in a secure MoJ facility.

Other tools

Some tools, such as Facebook, Instagram and LinkedIn, are approved for specific corporate accounts to use, for corporate communications messages. General use of these tools for work purposes is not permitted.

If you wish to use a tool that is not listed in this guidance, please consult our Guidance for using Open Internet Tools and ask for help.

Requesting that an app be approved for use

If there is an application or service that is not currently approved, but which you would like to use, you can request a security review.

Begin the request by filling in the Request a Security Review of a third-party service form, as best you can. The more information you provide, the better. But don't worry if you have to leave some bits of the form blank.

When you submit the form, it is passed to the security team. The app is reviewed, to check things like how safe it is to use, and whether there are any Data Privacy implications. The security team will respond to you with an answer as quickly as possible.

Note: You should submit the request, and wait for a formal "approval" response, *before* you install or use the app on MoJ equipment or information.

If you have any questions about the process, ask for help.

Other information
Government policy and guidance

GDS Social Media Playbook

NCSC

Video conferencing services: using them securely

Secure communications principles

Using third-party applications

Contact details

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

Phishing Guide

This guide provides information about 'phishing' is. It describes what phishing is, and how it happens. It tells you what you can do to protect yourself, and to keep Ministry of Justice (MoJ) systems secure.

There is also information on what to do if you think you have been phished.

What is a phish?

Phishing attacks are when threat actors pretend to be legitimate parties. They do this to steal money, credentials, or sensitive information. There are a variety of phishing attacks that you might come across. Some are more sophisticated or targeted than others.

Phishes often use two techniques:

- They affect emotional states.
- They create a sense of urgency.

Urgency makes users want to do the actions requested as quickly as possible. The combination of urgency and emotional manipulation leaves users feeling panicked and worried. It might fill them with a sense of euphoria. Threat actors use emotion and deadlines to convince users to act. The user doesn't take the time to think about whether it's a sensible or valid request.

Most phishes are emails, but they can also use other technology, such as SMS texts or telephone calls.

Threat actors might use phishes to request payments. They might ask you to click links and log in to an account or change a password. They might instruct you to buy items for them. They might get you to provide some personal details before you can claim a supposed prize. **Never** use the link in an email asking you to change a password. Use an out-of-band method such as going directly to the website to change a password. Be cautious when following password actions requested in emails or texts.

Threat actors utilise a variety of methods in phishes. They often take advantage of seasonal events to appear more legitimate. They use emotional and urgent triggers such as:

- Telling you that your tax return is overdue.
- Threatening to share access to your personal sensitive photos unless you pay.
- A request to send money urgently to a family member in trouble.
- Telling you 'good news' ,for example that you have won a big prize or are due a tax rebate.
- Providing a final demand about a very overdue invoice that, if unpaid, will see you taken to court.
- A 'last warning' about resetting your password, otherwise you will lose account access.

Beware of messages that create a sense of urgency or a heightened emotional state - good or bad. Treat such messages with suspicion. Check the message before you take any action. Unexpected messages with attachments are also common. Never open the attachment until you have done an out of band check.

Common types of phish

There are many different types of phish. You might recognise many of them. But the more sophisticated the phishing attack, the harder it is to spot. Out of band checks are the best way to stop a phishing attack. They use a second, different method of communication to check the authenticity of the contact and the requested action.

Email phishing

These are emails that request actions. Examples include clicking on links to change passwords, or requesting money. **Never** use the link in an email asking you to change a password. Use an out-of-band method such as going directly to the website to change a password. Be cautious when following password actions requested in emails or texts.

SMS phishing (smishing)

These are text messages that ask you to click links to access services or to pay for things. They often take advantage of seasonal events to appear more legitimate. Examples include Christmas delivery phishing texts, or texts around tax return time. Other recent examples use Covid news items to demand payments or personal information.

Voice phishing (vishing)

These are phone calls that ask you for sensitive information, or payments, or remote access to your devices. Threat actors might pretend to be from banks and other official organisations. Others might claim to be technology companies such as Microsoft. Another vishing example might claim to be from a jail, requesting bail money.

Spear phishing

Some phishing attacks focus on specific targets. Threat actors use OSINT to gather data about an individual. They can then create a 'custom phish'. It is interesting for the target. The target is then more likely to respond to the phish. Examples include real names or work-related jargon. These are often very sophisticated phishes. The use of personal data makes the phish more likely to succeed.

Whale phishing (whaling)

These target at high level individuals such as CEOs and Director level and above staff. Whaling uses a variety of phishing methods to contact high profile targets. The goal is to steal large sums of money, or access high level credentials, intellectual property, and sensitive information.

Business email compromise (BEC)

This type of phishing attack targets high level staff to steal money or reveal sensitive information. Threat actors pretend to be another high-level staff member. They do this by using their name or email address to seem legitimate. They often create a sense of urgency to convince junior staff to do the requested action. These emails often come from a compromised staff member's email account. This means the email system doesn't block the sender.

Watering hole attack

This is a very sophisticated supply chain attack. It uses research from an organisation's frequently used websites to identify a target. Targeted websites are then compromised and infected with malware. When users visit the websites, the malware downloads onto their systems. These are sophisticated attacks. The user is visiting an official and legitimate website. It is the website itself that has been compromised.

QR codes

Quick response codes (QR Codes) are a form of matrix (two-dimensional) barcode. They are machine-readable links. A QR code reader on a mobile device sends the user to a website or app. You don't need to click or type a link.

Some devices have QR code readers built into their camera app. Other devices need a dedicated app.

When you scan the QR code, the app asks you if you wish to go to the website or app described by the QR code.

Note: QR codes are not human readable. This means it is important to verify that the codes are legitimate and have not been tampered with.

You'll see QR codes in many situations. They give easy access to restaurant menus. They link to charity donation pages or surveys. Banks use them to link to services. They can be used to join wifi hotspots. They can be used to add contacts directly to your contacts list.

A QR code in an official context should be as safe to scan as an ordinary web link. For example, a QR code on an official notice in an MoJ building.

If the QR code is not labelled, or is from an unknown person, be suspicious. For example, a QR code stuck on a lamppost, or a QR code on a non-official flyer on a wall in a public location. These are not safe to scan.

It's possible that even a QR code in a safe, official place might be tampered with. Someone might draw over it. They might cover it with a sticker and a fresh QR code. If a QR code looks 'contaminated', don't scan it. Report it to security.

In summary, the risk associated with QR codes is currently considered low. They are simply barcode versions of web links. When deciding whether to scan a QR code or not, follow the same procedure as receiving an unexpected message .

Multi-factor authentication (MFA)

Multi-factor authentication (MFA) is a great way to reduce the risk of account compromise by a phishing attack. MFA provides an extra layer of defence for the account. If you have MFA set up, threat actors cannot access your account. It's safe, even if you accidentally reveal your credentials.

Never give MFA to codes to anyone. Genuine companies, banks, government departments, and social media sites will never contact you and ask you to tell them an MFA code. They will never offer to input it for you, or request you give the code to them over the phone. MFA codes should only ever be entered by you, directly into the account login.

MFA also provides an early warning system for credential compromise. If you ever receive an MFA code for an account that you are not actively logging into, then someone other than you is trying to access the account. This means your credentials might have been compromised, so as quickly as possible, you should:

- Report the problem to security.
- Change your password. **Never** use the link in an email asking you to change a password. Use an out-of-band method such as going directly to the website to change a password. Be cautious when following password actions requested in emails or texts.

Out of band checks

An out of band check is when an individual uses a different method of communication than the one the message came from. This method means that if one communication method is compromised, you quickly find out by using a different communication method to confirm validity. The likelihood of multiple communication methods for the same person or team being compromised is low.

Out of band checks are an easy method to confirm the legitimacy of communications and requests. They can confirm the identity behind a message or request, and they can confirm the validity of the message or request itself. Social engineering techniques and phishing tactics take advantage of people who do not use out of band checks. By doing an out of band check, these sorts of attacks can be stopped very easily.

Example 1: You receive an email request for an urgent review of an invoice, and immediate payment. The email comes from someone unexpected. You should find the official contact details of that person, and contact them using a phone call - but not email - to confirm that they did indeed send the original email. If they did send the email, you can

proceed with the request. If they did not send the email, you can report the email as a phish, and also alert the owner of the email address that their email address might have been compromised.

Example 2: You receive a phone call from someone claiming to be your bank, or HMRC, or HMCTS. You hang up the call, and locate the official website for the company. You should be able to find multiple official contact details there. Use one of these to contact the place the caller claimed to be from. If, for example, the claim was that your bank was calling, you can call the direct number and speak to the switchboard about the reason for the initial call. They will forward you to the correct department. You can then confirm the validity of the original call, and so confirm whether the original caller was actually from your bank or not.

Example 3: Someone enters your place of work, and claims to have a meeting with a specific person. Unfortunately, there is no record of this on the expected visitor list. You can call or email the person within your place of work to confirm the visitor is legitimate. This check also works if tradespeople arrive unexpectedly, because you can contact both the relevant person within your place of work and also contact the company they claim to be from, using the company's official website contact details.

Example 4: You receive an email requesting that you reset your password immediately. The email contains a link to perform the password reset. You have not attempted to login to that account recently. You should use an internet search for the website or type the URL directly if you know exactly what it should be. When you attempt to login, the website will let you know if you need to reset your password. If not, you know someone else has attempted to gain access to your account. That would mean the password reset request was not legitimate, and most likely a phishing attempt hoping to get your username and password through the reset link in the original email. Similarly, if you get an MFA request unexpectedly, do not confirm it unless you were indeed attempting to access that account immediately before the request came through. If you get an MFA request, but had not been trying to connect using the account, you should change the account password as soon as possible, because it might have been compromised.

When doing an out of band check, be sure to pick a different method of communication to the one used to contact you originally. If someone emails you unexpectedly, perform an out of band check by making a phone call. If someone calls you, perform an out of band check by using the Internet. It is very unlikely that multiple communication channels have been compromised.

Be sure to get official contact details for companies only from their official websites. Never be afraid to hang up on someone and check their identity through another method, especially if they are asking for sensitive or personal information or credentials. Never be afraid to check the legitimacy of unusual email requests. by contacting the sender through a different communication channel.

Doing an out of band check lets you confirm that the messages come from the person they claim to be, and that the requests are valid. This helps prevent you or your company from losing money to fake invoices, from accidentally giving up sensitive information or credentials, and from having unauthorised individuals in your place of work. Doing an out of band check is fast and easy.

All members of your workplace should be happy to receive such a check. It shows that you take security seriously, and that you are helping to protect them as well as yourself.

If you think you've been phished

Don't panic.

You will not be punished if you fall for a phish - it can happen to anyone. You will not be punished for reporting a phish, even if it turns out to be a false alarm.

If you think you have been phished:

1. Report it immediately.
2. If your credentials were phished, highlight that in the report.
3. Change the password for affected accounts as soon as possible. **Never** use the link in an email asking you to change a password. Use an out-of-band method such as going directly to the website to change a password. Be cautious when following password actions requested in emails or texts.

MoJ firewalls and antivirus systems should catch the majority of malware before they can affect systems. By reporting the incident as quickly as possible, the security team will be alerted and on the lookout for any more sophisticated malware.

If your credentials have been phished, reporting it immediately and resetting your password quickly greatly reduces the risks.

Any phishing emails that get through the filters and into your inbox will be very sophisticated. This makes them much harder for you or anyone to spot. Never feel guilty or ashamed for being phished.

Reporting phishes

Reporting phishing attempts helps improve the filters that catch them before they get to your inbox. They also help protect other colleagues and the MoJ from being compromised, or having data or money stolen.

If you think you have spotted a phish, or you think you have been phished, report it as quickly as possible. If you think you have spotted a more targeted phish that claims to be from a vendor or another staff member, do an out of band check to determine if it is legitimate. If it is not, then please report the email as a phish.

Reporting a phishing attempt is quick and easy. Contact service desk using one of these two options:

- Tel: 0800 917 5148
- MoJ Service Portal and Live Chat

You can also forward on all spam and phishing text messages to 7726 for free.

Contact details

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

Protecting WhatsApp accounts

The Ministry of Justice (MoJ) permits the use of WhatsApp for text messaging, voice and video calls. You **should** avoid using it for business tasks involving personal or sensitive data.

You **should** always keep WhatsApp account details safe and secure. Accounts link with specific devices. When you register your device with a WhatsApp account, that provides some protection. Only the registered device can send or receive messages associated with you.

Unfortunately, device registration is a tempting target for attackers. It is a way for potential compromise of user data. Compromises affect backups of conversations, and contact lists.

A compromised account might also attack other people. An attacker might pretend to be a user, and so target other contacts. They might make their way to compromise a high-value target.

An example scenario might be an attack on the WhatsApp account of a family member of an MoJ employee. The attacker compromises the family member’s WhatsApp account. They then pretend to be the family member. They contact the MoJ employee through the contact list. The employee trusts the message: it seems to come from the family member.

How a WhatsApp attack works

Note: This document does not provide full details of how to attack a WhatsApp account. We provide enough information to understand helpful protective steps.

Registering a device with a WhatsApp account uses an authentication code (a PIN code). The attacker tricks the victim into revealing the device registration code. They then deregister the victim's device from the WhatsApp account. Next, they register the attacker's device with the WhatsApp account.

The key point is the authentication code. It's very important to keep this secret, like a password.

Recovering and protecting your WhatsApp account

You can often recover a compromised WhatsApp account. A good way is to use your device telephone number. Use the app to ask for a 6-digit SMS verification code. When the code gets to your phone, enter it into the app. After re-authenticating your phone, the attacker is automatically disconnected. They cannot reconnect without a fresh authentication code.

While recovering an account, you might have to provide a two-step verification PIN. If you don't have this code, it suggests the attacker enabled two-step verification. Without the code, you must wait 7 days before you can sign in to WhatsApp. But the attacker is disconnected from the account immediately when the code is sent. Although you can't get into your account for a week, the attacker cannot get into your account at all.

When you reconnect into your WhatsApp account, check for any unknown devices. Do this by checking **Linked Devices** in the WhatsApp settings menu.

Always enable two-step verification on your account. Any future attempt to register a device needs a PIN to enable the app. Do this by going into the **Settings** then **Account** menu on the app. Select the **Two-step verification option**.

If there's something suspicious about your MoJ account, or the messages in the account, contact the MoJ Security team. Ask for help as soon as possible.

Always follow MoJ policy about applications for official business or storing business-related information. Don't use unapproved applications for MoJ official business. Don't use unapproved applications for storing MoJ business-related data. Always use approved applications and storage tools.

WhatsApp account do's and dont's

Do ask Security team for help if you think your WhatsApp account has been compromised.

Do enable two-step verification on your account. Do this by going into the **Settings** then **Account** menu on the app. Select the **Two-step verification option**.

Do tell everyone on your contact list if you think your WhatsApp account has been compromised.

Do check the list of linked devices at regular intervals. Look for unknown or unexpected devices. Do this by checking **Linked Devices** in the WhatsApp settings menu.

Do not share a WhatsApp one time passcode, password, or authentication code with anyone.

Do not use unapproved or unauthorised applications for work purposes.

Do not use personal accounts for work purposes.

Contact details

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

Secure Data Transfer Guide

Introduction

This guide outlines the security procedures and advice for Ministry of Justice (MoJ) staff wanting to send or receive data securely from external sources.

This is important to the MoJ, because personal and sensitive data is regularly transmitted between departments. Legislation such as GDPR, and industry standards such as PCI DSS, affect the MoJ's responsibility to secure this data. It is also important to recognise the damage that leaked sensitive data could cause to the vulnerable people the MoJ works to protect.

Who is this for?

This policy is aimed at three audiences:

1. **Technical users**: these are in-house MoJ Digital and Technology staff who are responsible for implementing controls during 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.

2. **Service Providers**: defined as any other MoJ business group, agency, contractor, IT supplier, or partner who in any way designs, develops, or supplies services (including processing, transmitting, storing data) for, or on behalf of, the MoJ.
3. **General users**: all other staff working for the MoJ.

The phrase "all MoJ users" refers to General users, Technical users, and Service Providers as defined previously.

Transfer Considerations

Anyone handling personal or sensitive data must seek consent from their line manager to authorise data transfer.

Before any data transfers are requested, consider the following:

- Is it strictly necessary for the effective running of the MoJ, and the care of the people it serves, that the data (regardless of whether the data is sensitive or not) is transferred?
- What is the nature of the information, its sensitivity, confidentiality, or possible value?
- What is the size of the data being transferred?
- What damage or distress might be caused to individuals as a result of any loss or unmanaged sharing during transfer?
- What implications would any loss or unmanaged sharing have for the MoJ?
- What information is actually necessary for the identified purpose? For example, is the intention to send an entire document or spreadsheet, when only one section, or specific spreadsheet columns, are required?
- Has the identity and authorisation of the information recipient been established?

Any transfer technique used **shall**:

- Encrypt the data over the network (in transit), using sufficient and appropriate encryption (currently TLS 1.2 or greater).
- Require strong authentication to ensure that both the sender and recipient are who they claim to be.

These considerations apply when transmitting any data over a wireless communication network (for example wifi), or when the data will or might pass through an untrusted network.

If the MoJ is the controller of the data being transferred, the security storage requirements at the destination **shall** be considered to ensure that they comply fully with the relevant regulation, such as PCI DSS or GDPR.

If it's not clear who the data controller is, ask the Data Protection Team for help.

When dealing with third parties, consider whether any data sharing agreements or contracts are in place that apply to the transfer of that data. Check whether there are any stipulations in place regarding the method of transfer that can or should be used.

If personal data is being transferred to a third party, then the privacy team **shall** be informed, to decide if a Data Protection Impact Assessment is required.

Data Transfer

Normally, files **should not** be transferred by email. Normally, files **should** be transferred by secure network links using appropriate protocols such as `https`, `ssh`, or `sftp`. For large files, such as those over 5MB, transfer using a secure protocol is a practical necessity, as many recipients will not accept emails with attachments greater than 5MB.

Data Transfer by Secure link

The MoJ's preferred method of data sharing is to use Microsoft Teams via Sharepoint. Teams has been authorised to hold **Official-Sensitive** information. It is configured to provide greater granular protection through tools such as Azure Information Protection (AIP). Where possible, data **should** be transferred using Teams.

Due to the diverse nature of the MoJ's architecture, using Teams might not always be possible. Those in the MoJ Digital and Technology team who do not have access to Microsoft Teams **may** use Google Workspace to transfer data.

For more details on the actual process for a transfer, contact the Security team.

Data Transfer by email

Where it is not possible to use Microsoft Teams or Google Workspace, **AND** the data to be transferred is less than 20MB, email **can** be used, **BUT** the following requirements **shall** be met:

- Email communication **should not** be used to transfer unencrypted sensitive or personal data. Employees **should** note that emails are not designed to attach and transfer large amounts of data. The MoJ's email system does not support file attachments that exceed a total of 20MB.
- You **should** consider an alternative secure method of transferring sensitive data wherever possible and practicable. If no suitable alternative is available, then apply an extra level of security. Do this by using encryption to apply a strong password to the sensitive data you wish to send. All passwords **shall** be transferred using an alternative method of communication to get to the recipient. Examples includes post, a telephone call to an agreed number, or by SMS text message.
- Email messages **shall** contain clear instructions of the recipient's responsibilities, and instructions on what to do if they are not the correct recipient.
- Information sent **shall**, where practical, be enclosed in an encrypted attachment.
- Care **shall** be taken as to what information is placed in the subject line of the email, or in the accompanying message. Filenames or subject lines **shall not** reveal the contents of attachments. Filenames or subject lines **shall not** disclose any sensitive personal data.
- Emails **shall** only be sent from your work email address, as provided by the MoJ. This is to ensure that the correct privacy and security information is displayed.

CJSM email

- The Criminal Justice Secure email Service (CJSM) is provided for criminal justice agencies and practitioners to communicate with each other.
- As a general rule, it **shall** only be used for purposes relating to the criminal justice service.

Microsoft 365 Encrypted email

- This facility is available for standard individual and generic MoJ email accounts
- This method **can** be used to send or receive files classified as **Official**. It is normally used with external partners, agencies, or individuals who cannot be contacted using CJSM email.
- The attached files on a single email **can not** exceed 25MB.

Removable storage devices

The MoJ strongly discourages the use of removable storage devices such as USB devices for data transfer. However, if all other options are not possible, then removable storage devices **may** be used with caution.

Any data being transferred by removable media such as a USB memory stick **shall** be encrypted. Encrypted portable storage devices **shall** be password protected with a strong password. All passwords **shall** be transferred using an alternative method of communication to get to the recipient. Examples includes post, a telephone call to an agreed number, or by SMS text message.

If you think you have no other option for copying or moving data, and have to use removable media, contact the Security team.

Ownership of any removable media used **shall** be established. The removable media **shall** be returned to the owner on completion of the transfer. The transferred data **shall** be securely erased from the storage device after transfer.

Clear instructions of the recipient's responsibilities, and instructions on what to do if they are not the intended recipient, **shall** accompany the removable media.

Any accompanying message or filename **shall not** reveal the contents of the encrypted file. The sender **shall** check, at an appropriate time, that the transfer has been successful, and obtain a receipt. An email confirming receipt is acceptable.

Report any issues to your line manager and in the case of missing or corrupt data to the Security team immediately.

Data transfers by post or courier

Data transfers using physical media such as memory cards or USB devices **shall** only be sent using secure post. Royal Mail First or Second class **shall not** be used. Royal Mail Special Delivery or Recorded Delivery **can** be used. For non-Royal Mail services, a secure courier service **shall** be used, with a signature obtained upon delivery. The recipient **shall** be clearly stated on the parcel. The physical media **shall** be securely packaged so that it is not damaged in transit.

The recipient **should** be told in advance that the data is being sent, so that they know when to expect the data. The recipient **shall** confirm safe receipt as soon as the data arrives. The sender responsible for sending the data is also responsible for confirming the data has arrived safely.

Hand Delivery and Collection

Hand delivery or collection of data **may** be used where removable media is used. When arranging for an individual to collect information, the identity of the individual **shall** be established, to confirm who they claim to be. An appropriate form of identification **shall** be provided before handing over any documentation.

Telephone or Mobile Phone

Phone calls might be monitored, overheard, or intercepted. This might happen deliberately or accidentally. Take care to protect calls, as follows:

- Transferred information **shall** be kept to a minimum.
- Personal or Confidential information **shall not** be transferred over the telephone, unless the identity and authorisation of the receiver has been appropriately confirmed.

Residual risks with encrypted data transfer

All users **should** recognise that even if a system uses encrypted data transfer, there are still occasions where data might be affected by unauthorised access. Be aware of these residual risks. Line Managers **should** include consideration of these risks in employee awareness training. Examples include:

- Some data relating to the communication might still be exposed in an unencrypted form. An example is metadata.
- Data transfer processes that rely on Public Key Infrastructure (PKI) **shall** implement strict certificate checking to maintain trust in end-points.

Incidents and contact details

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

For help with incidents, including theft and loss, contact one of the following:

Technology Service Desk - including DOM1/Mojo, and Digital & Technology Digital Service Desk. Use one of the following two methods for contacting service desk:

- Tel: 0800 917 5148
- MoJ Service Portal and Live Chat

Note: The previous `itservicedesk@justice.gov.uk` and `servicedesk@digital.justice.gov.uk` email addresses, and the Digital & Technology Digital Service Desk Slack channel (`#digitalservicedesk`), are no longer being monitored.

HMPPS Information & security:

- Email: informationmgmtsecurity@justice.gov.uk
- Tel: 0203 334 0324

For non-technology incidents, contact the Security team

Contact the Data Protection Team for information on Data Protection Impact Assessments: DataProtection@justice.gov.uk

If you are not sure who to contact, ask the Security Team:

- Email: security@justice.gov.uk

- Slack: `#security`

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

Sending information securely

This guidance complements the Ministry of Justice (MoJ) overall security policy.

This guidance on working securely with paper documents and files applies to all employees, contractors, partners and service providers, including those on co-located sites and sites owned by other public bodies. This also includes employees of other organisations who are based in, or work at, MoJ occupied premises.

Agencies and arm's length bodies (ALBs) are expected to comply with this corporate framework but may establish their own arrangements tailored to operational needs and should supplement it with local policy or guidance for any business-specific risk.

Related information

IT Security Policy (Overview) on page 17

Objective

The MoJ requires employees and contractors to get into the habit of looking after the information that they work with, whether it's on paper or stored electronically, in the same way they would take care of their personal valuables.

Scope and Definition

This guidance helps you understand the risks involved in sending information. It covers any information that relates to the business of the MoJ, its stakeholders and partners that have been printed out or written down on paper, and information that has been downloaded from IT systems onto 'removable media'.

This guidance outlines the all the basic guidance on sending information using email, post, courier services and fax.

Context

All MoJ information is valuable, and staff are expected to protect everything that relates to the department's business, including information provided by others. This applies to all information, not just information that is covered by the Data Protection Act or classified under the Government Classification Scheme.

There are different rules for managing and protecting different kinds of paper-based information. You need to know how to:

- Identify the correct security level for the information you work with.
- Handle it according to the relevant rules.

Responsibilities

All employees, contractors, partners, service providers and employees of other organisations who are on MoJ premises and co-located sites remain accountable for the security, health and safety of themselves, colleagues and the protection of departmental assets.

Policy statements

Using email

Email is the preferred option for securely transferring information between yourself and another civil servant. You **shall** use departmental equipment and transfer between **Official** or CJSM email accounts.

If the person or organisation you are sending the information to is outside departmental **Official** or CJSM networks, you **shall** consider the sensitivity of the information. It might be safer to send it on encrypted removable media or in hardcopy.

Sending bulk information

Transferring bulk data **shall** be authorised by a senior manager.

The definition of bulk or high volume is not specific. Removable media such as laptops, disks or memory sticks can hold thousands of records. They have the benefit of encryption to prevent access to data accessed, but the damage if

they are lost and the information cannot be retrieved remains high. However, information is immediately accessible if even a single paper files is lost, so the risks need to be managed differently.

As an indication, datasets containing the electronic records of 1,000 or more people would count as bulk, whilst decisions on using more secure forms of movement might apply to much smaller volumes of case files. It might also apply to lesser volumes where names and addresses are combined with sensitive information that might lead to identification.

In all cases, consideration **shall** be given to the risk and impact of causing individuals or the MoJ to suffer harm or loss, service disruption, or reputational damage.

Using post and couriers

There are a range of methods of sending documents, depending on the potential harm that result from loss. This relates to their security classification and the volumes involved. Use a method that is appropriate for the type of information:

- For normal inter-office transit, use DX delivery services or agreed contracts for the movement of papers or files. Royal Mail letter post is otherwise acceptable for standard non-sensitive material, or letters at **Official**.
- The classification and any handling caveat such as **Official-Sensitive shall not** be shown on the outer envelope. If the contents are sensitive, particularly if they contain personal details intended for an individual, the envelope **should** be marked `ADDRESSEE ONLY`. Post rooms **shall** check addressee details, and **shall not** open any envelope marked in this way.
- If more security is needed, either because material is being sent in bulk or the contents are more sensitive, tracked options including tracked DX or special delivery **should** be used.
- Material marked **Official-Sensitive can** be sent using any of the previous methods, with a return address and no protection marking on the outer envelope.
- Double enveloping might also provide additional protection, especially if there is a risk the package might burst or if it is being sent to a non-MoJ location where the `ADDRESSEE ONLY` instruction might not be recognised.

Confirming delivery

If you are sending sensitive or bulk information, you **shall** ensure that the recipient is expecting it and get confirmation of receipt. Consider a solution that allows you to track delivery. If you need to transfer or send personal data to or outside of the European area, discuss it first with the Data Protection Team.

Faxing documents between sites

Office faxes **shall** only be used for transmission and exchange of MoJ information where other more secure means of communication, for example **Official** government email, are not possible.

Where use of fax machines (including Goldfax where available) remains the best option, it **shall** only be for information classified at **Official** and that is not especially sensitive. The reason is that fax material is sent over public networks. Faxed information might be individual items, including personal data.

Bulk transmission of personal data and information marked **Official-Sensitive shall** only be allowed following a risk assessment and approval from the Information Asset Owner.

The following controls and procedures **shall** also be applied by staff:

- Ensure that the recipient has a legitimate need to access department information for official business purposes.
- Take care to ensure that the correct number has been dialled, and that the authorised recipient is attending the receiving fax terminal at the time the information is being faxed.
- Immediately contact the authorised recipient to authenticate that they have received the information, verifying the quantity (the number of pages), and content of the information.
- If the recipient's fax line is busy and a transmission is not possible, wait until it is free. Do not leave the fax machine unattended. You **shall** confirm that the authorised recipient has received all the information.
- Each transmission should carry the following:
    - A unique reference number.
    - The identity of the originator.
    - The identity of the intended recipient.

    - A record of the number of pages transmitted.
- Ensure that the authorised recipient is aware of the handling requirements for **Official** information, including preventing information being viewed or accessed by unauthorised persons in their business.
- If the fax is configured to produce a confirmation of transmission report, including a copy of the first page of the transmission, ensure that you retain this hardcopy information and that it is not left on the fax machine where it might be seen by those who do not 'need to know'.
- Ensure that the fax is configured correctly, and that functions such as polling reception (programming to send messages to specific numbers), redirection, forwarding, and remote control are disabled.

Overview of threats and vulnerabilities

The public service telephone networks through which fax messages are transmitted are exposed to several significant security vulnerabilities and threats. These include:

- The potential that even UK to UK transmission is routed to overseas networks, increasing risks.
- Transmission within the UK may be intercepted at several places along the route.

In addition, the risks associated with fax machines are as follows:

- Unauthorised access to the built-in message stores to retrieve messages.
- Deliberate or accidental programming of machines to send messages to specific numbers.
- Sending documents and messages to the wrong number, either by misdialling, or by using the wrong stored message.
- Viewing of protectively marked messages by unauthorised persons, for example copies left unattended and unsecured on fax machines and traffic logs, and copies of fax messages retained on the machine's memory being accessed.

What to do if you think there has been a security breach

If you suspect that the security of the information you work with has been compromised in any way, you **should** report it immediately. A security breach doesn't have to involve the actual loss of information. The potential loss of information also counts.

For example, if a security cabinet has been left unsecured, there might be no evidence that any information has been lost or interfered with, but there is a clear potential for loss or damage.

Compliance

The level of risk and potential impact to MoJ assets and most importantly physical harm to our people and the public determines the controls to be applied and the degree of assurance required. The MoJ **shall** ensure that a baseline of physical security measures are in place at each site, and receive annual assurance that such measures are in place to provide appropriate protection to all occupants and assets, and that these measures can be strengthened when required, for example in response to a security incident or a change in the Government Response Level.

The implementation of all security measures **shall** be able to provide evidence that the selection was made in accordance with the appropriate information security standards ISO27001/27002, and with Physical Security advice taken from the Centre for the Protection of National Infrastructure (CPNI) and Government Functional Standard - GovS 007: Security (link is external).

The constantly changing security landscape has necessarily dictated that Physical Security measures be constantly re-evaluated and tested in order to meet new threats and other emerging vulnerabilities. This policy and subsequent supporting standards are subject to annual review or more frequently if warranted.

Physical security advice

Physical security advice can be obtained by contacting Security team.

Annex A: Suitable carriers

This guidance does not provide an exhaustive list of suitable carriers but does identify recommended options. The following notes provide further details.

Royal Mail

Ordinary letter post is acceptable for **Official** correspondence with members of the public or items that must be sent to private addresses. To prevent inappropriate opening of personal letters with sensitive personal data sent internally or to other business addresses, you **should** mark the envelope 'addressee only'. This might also require double enveloping to protect the contents in transit, and prevent inappropriate opening on delivery.

Recorded delivery

Recorded delivery **should** be used if the letter contains particularly sensitive information or identity documentation. The sender is given a reference and can confirm delivery and obtain a copy of the signature through the Royal Mail website.

Special delivery

This is similar to recorded delivery, but requires a named signature for receipt. Earlier delivery can be arranged (9am or 1pm). This service also allows online tracking of the item, suitable for more sensitive documents.

For more information, refer to the "Courier and postal services Royal Mail" document available on MoJ MyHub (log in to MyHub and use the search facility to locate the document).

DX

Ordinary DX services are acceptable for sending low volumes of files or enveloped papers between sites and other justice agency partners with registered DX addresses. When sending any volume or sensitive papers, managers **should** ensure that the receiving office is expecting the delivery, and check receipt.

Tracked DX

This is recommended when a more formal tracking is required, either because of the volumes of files, or because they contain particularly sensitive case information.

There two further DX options which give added security:

- Courier Tracked.
- Secure DX.

For more information, refer to the "Courier Services Document Exchange and Next Day – DX Network Services" document available on MoJ MyHub (log in to MyHub and use the search facility to locate the document).

You can also use tracked courier services provided by FedEx.

Contact details

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

Web Browsing

The Ministry of Justice (MoJ) provides access to the Intranet and Internet for business use. The access helps you to do your job effectively and efficiently.

MoJ security policies governs your use of these facilities.

Reasonable personal use is allowed, if:

- Your line manager agrees.
- It does not interfere with the performance of your duties.

You and your manager are responsible for ensuring that you use these systems responsibly.

If you connect to a website that contains unsuitable, illegal or offensive material:

- Disconnect from the site immediately.
- Inform your IT Service Desk.

The Department monitors the use of electronic communications and web-browsing activity. If your email use or web browsing seems unacceptable, your manager can request detailed activity reports.

What websites you can access

The MoJ's approach to website access is continually reviewed and updated. By default, we try to allow access to as much as possible of the internet for all users. Inevitably, there are some restrictions, for the following reasons:

Cyber Security

- The site is an unacceptable security risk for MoJ systems or users. For example, sites known to host malware are blocked.

Technical

- The site causes technical issues which interfere with business activities. For example, a video site uses too much network capacity.

Business Policy

- Only a specific individual or group of users can access the site. For example, social media sites are blocked for systems or users in frontline roles.

The list of websites included in each of the categories is as small as possible. But if you cannot access a site that you think should be OK, you can request a review. Similarly, if you can access a site that you think should be blocked, request a review.

What to do if you are blocked from a website that you think should be OK

Log an incident with your IT Service Desk.

Provide the following details:

- The address of the website.
- The time you visited the site.
- The details of any block message that you received.

The IT Service Desk will investigate the reason why you cannot access the website.

If there was a system error or fault, remedial action will restore access.

If the block is due to an access rule, the Security team reviews whether to change the rule.

What to do if you are able to access a website that you think should be blocked

Log an incident with your IT Service Desk.

Provide the following details:

- The address of the website.
- The time you visited the site.
- The reason why you think the site should be blocked.

Other help

- HMPPS Prison - All requests should be directed to the IT Service Desk via a local or area IT Manager.
- HMPPS Probation - Log an incident with your IT Service Desk.
- All other teams, contact the Security team.

General enquiries, including theft and loss

Technology Service Desk - including DOM1/Mojo, and Digital & Technology Digital Service Desk. Use one of the following two methods for contacting service desk:

- Tel: 0800 917 5148
- MoJ Service Portal and Live Chat

Note: The previous `itservicedesk@justice.gov.uk` and `servicedesk@digital.justice.gov.uk` email addresses, and the Digital & Technology Digital Service Desk Slack channel (`#digitalservicedesk`), are no longer being monitored.

HMPPS Information & security:

- Email: informationmgmtsecurity@justice.gov.uk
- Tel: 0203 334 0324

Web browsing security policy profiles

There are two policy profiles, one for the Judiciary, and one for all other staff.

Each profile identifies categories of content that are normally blocked. Content that is not in a blocked category will normally be available to a profile.

Judiciary

All activity is logged. By default, no reporting takes place. However, reporting is permitted following appropriate judicial sanction.

The following categories of content are normally blocked for the Judicial profile:

- Advanced Malware Command and Control
- Advanced Malware Payloads
- Botnets
- Compromised Websites
- Custom-Encrypted Uploads
- Dynamic DNS
- Elevated Exposure
- Emerging Exploits
- Extended Protection
- Files Containing Passwords
- Keyloggers
- Malicious Embedded iFrame
- Malicious Embedded Link
- Malicious Websites
- Mobile Malware
- Newly Registered Websites
- Phishing and Other Frauds
- Potentially Exploited Documents
- Potentially Unwanted Software
- Security
- Sex
- Spyware
- Suspicious Content
- Suspicious Embedded Link
- Unauthorised Mobile Marketplaces
- User-Defined list

All other staff

Limited restrictions are in place to block web access. All activity is logged. Reporting is enabled for all activity.

The following categories of content are blocked for this profile:

- Adult Content
- Adult Material
- Advanced Malware Command and Control

- Advanced Malware Payloads
- Application and Software Download
- Botnets
- Compromised Websites
- Custom-Encrypted Uploads
- Dynamic DNS
- Elevated Exposure
- Emerging Exploits
- Extended Protection
- Files Containing Passwords
- Keyloggers
- Malicious Embedded iFrame
- Malicious Embedded Link
- Malicious Websites
- Mobile Malware
- Newly Registered Websites
- Phishing and Other Frauds
- Potentially Exploited Documents
- Potentially Unwanted Software
- Security
- Sex
- Spyware
- Suspicious Content
- Suspicious Embedded Link
- Unauthorised Mobile Marketplaces
- User-Defined list

Wifi security policy

Introduction

This policy gives an overview of wireless networking (wifi) security principles and responsibilities within the Ministry of Justice (MoJ).

To help identify formal policy statements, each is prefixed with an identifier of the form: **POL.WIFI.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.

Purpose

The purpose of this document is to define a set of security requirements for MoJ wifi networks, based on industry good practices and our local requirements.

POL.WIFI.001: Any exceptions to the policy **shall** be managed through the MoJ's security risk management process.

Applicability

This policy applies to all MoJ owned or managed wifi networks provided for any purpose. It also applies to the use of third-party wifi networks by MoJ devices which handle **Official** information, for example staff end user computing devices.

MoJ wifi networks

POL.WIFI.002: Each MoJ wifi network **shall** have a defined policy which is reviewed at least annually, that describes:

- The purpose of the wifi network.
- The intended users of the wifi network.
- The Service Owner of the wifi network.
- The access controls that are applied to ensure that only those intended users can connect to the wifi network.
- User and administrator responsibilities for maintaining the security of the wifi network.
- Who has authority to expand or alter the wifi network.
- Logging and monitoring requirements and responsibilities for the wifi network.

General security requirements

The following statements apply to all MoJ-provided wifi networks.

POL.WIFI.003: Wifi networks **shall not** be treated as extensions of trusted LANs or WANs.

POL.WIFI.004: Wifi networks **shall** be treated as untrusted bearers for the purposes of application security.

POL.WIFI.005: All products used in an MoJ wifi network **shall** support WPA2-Enterprise.

POL.WIFI.006: CCMP **shall** be used to protect the confidentiality and integrity of information transmitted over the wifi network.

POL.WIFI.007: Other wifi security modes (such as WEP) **shall not** be enabled.

POL.WIFI.008: All products used in MoJ wifi networks **shall** support certificate-based authentication.

POL.WIFI.009: On MoJ wireless networks, isolation between wifi clients **should** be enabled. Where there is no requirement for devices to communicate directly, isolation **shall** be enabled.

POL.WIFI.010: MoJ wireless networks **should** use a DNS resolver that chains to the Protective Domain Name Service (PDNS) service.

POL.WIFI.011: All MoJ wireless networking equipment **shall** be kept patched and secure, whether connecting to MoJ wifi services or GovWifi.

POL.WIFI.012: All management of MoJ Wireless networking equipment **shall** be undertaken in compliance with the Privileged User Access Guide and any relevant Security Operating Procedures (SyOPS).

MoJ enterprise wifi networks

Note: MoJ enterprise wifi networks are those used solely for MoJ users and devices.

POL.WIFI.013: Pre-Shared Keys (PSKs) **may** be used for user or device authentication.

POL.WIFI.014: PSKs **shall** be unique per user or device.

POL.WIFI.030: For MoJ guest wifi networks, but not including GovWifi, audit logs of sites accessed **shall** be retained for at least 6 months, including authentication details. This data is held to allow forensic analysis of data in the case of a security incident. No personal information except that required to conduct the analysis is logged or retained.

Using third-party wifi

POL.WIFI.031: MoJ staff **shall** ensure they have permission from the network owner before using wifi that is not operated by the MoJ.

POL.WIFI.032: Staff **should** take reasonable precautions to check that their home wifi network is secure.

POL.WIFI.033: Staff **may** use work-provided mobile phones to 'tether' their MoJ-provided devices for connectivity.

POL.WIFI.034: Tethered connections **shall** be password protected using unique and complex passwords.

POL.WIFI.035: Tethering passwords for MoJ devices **shall not** be shared with non-MoJ users.

POL.WIFI.036: Public wifi networks or guest wifi provided at third-party sites **shall** only be used by devices which have suitable encryption for MoJ **Official** information. Here, 'suitable' means either an 'always-on full-take' VPN, or that provides appropriate application-level encryption for all services. This is currently (October 2021) limited to Dom1 and PTTP/MoJO laptops and mobile devices.

POL.WIFI.037: Staff travelling overseas **shall** follow the guidance on accessing MoJ IT systems from overseas regarding the use of wifi or other networks.

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.

Information security incident management

Management of information security incidents and improvements

IT Security Incident Management Policy

How to use this policy

This policy is for all users and is part of a set of Ministry of Justice (MoJ) policies and supporting guides that cover various aspects of incident and disaster management and response.

The policies are:

- IT Security Incident Management Policy
- IT Disaster Recovery Policy
- IT Investigations - Planning and Operations Policy

The supporting guides are:

- IT Incident Response Plan and Process Guide
- IT Disaster Recovery Plan and Process Guide

This policy describes what is needed to manage an IT Security Incident.

Information is listed beneath the following headings:

- Policy statements
- What is IT Security Management?
- Definition of an IT Security incident
- Types of incidents
- Incident detection and reporting
- Incident categories
- Escalations
- Incident management stakeholders
- Investigations
- System recovery
- Lessons learned

MoJ Security Team

In this policy, 'MoJ Security Team' refers to all the security teams within the MoJ.

The MoJ Security Team are responsible for:

- incident ownership, monitoring, tracking and communication
- sanctioning enhanced monitoring where appropriate
- updating the incident management database
- analysing security incidents as required
- initiating a forensic investigation
- providing progress reports to relevant parties

To contact the MoJ Security Team, send an email to security@justice.gov.uk.

Policy statements

This policy refers to the Policy Statements, **POL.IMP.001** to **POL.IMP.014**.

POL.IMP.XXX indicates the specific policy statement to be adhered to.

What is IT security management?

IT Security Incident management is the ability to react to MoJ IT security incidents in a controlled, pre-planned manner.

Preparation and planning are key factors to successful information security management. This policy sets out good practice for dealing with IT security incidents.

Definition of an IT Security Incident

A security incident is defined by the National Cyber Security Centre (NCSC) as:

- a breach of an IT system's security policy in order to affect its integrity or availability
- the unauthorised access or attempted access to an IT system

An IT incident may result in sensitive information being exposed, which might compromise MoJ business delivery or the Data Protection Act.

An incident might also cause harm or damage to individuals or organisations and result in operational disruption or reputational damage to the MoJ.

All MoJ staff **shall** be aware of the definition of a security incident and how to report it.

Incident Response

An incident response is the action taken when a security incident is detected or reported.

Responding to an incident requires informed decisions, taken as part of a consistent approach that is designed to reduce the consequences of the incident.

The process to respond to an incident **should** be described in detail in an Incident Response Plan.

POL.IMP.001: Each MoJ IT system and service **shall** have an IT Security Incident Response Plan.

The IT Incident Response Plan and Process Guide has information on what to include in a Response Plan.

Types of Incidents

Types of IT Security related incidents include:

- breaches of the IT Security Acceptable Use Policy
- detection of malicious code such as viruses and malware
- network attacks or Denial of Service (DOS) attacks
- scanning and probing of a network, which might consume significant network resources
- the discovery of a new network vulnerability
- release of a patch or software update which is considered critical or an emergency
- a penetration test on a live operational IT system that reveals critical vulnerabilities
- unauthorised access to an MoJ IT system
- personal data incident due to accidental or deliberate loss or release of personal information
- any alert or activity report generated by an MoJ IT system that proves to be a real security alert

Incident Detection and Reporting

Security incidents may be discovered by:

- protective monitoring solutions
- incident reports by MoJ staff
- third-party reports to the MoJ
- breaches of MoJ IT Security Policy detected by an IT system
- data surrounding IT security incidents or suspected IT security incidents can be captured and monitored for suspected malicious activity or breaches of security

POL.IMP.002: All MoJ IT Security incidents or suspected incidents **shall** be reported to the IT Service Desk as soon as they are identified.

POL.IMP.003: All MoJ IT Security incidents involving personal data **shall** be reported to the MoJ Data Protection Team.

The MoJ Security Team is responsible for maintaining a database of IT Security incidents across MoJ IT systems.

This database contains:

- security incident reports
- the status of all reported security incidents and any actions taken to mitigate them

Further guidance on how to report a security incident.

Incident Categories

Security incidents are categorised to assess their impact and required level of escalation.

The three categories are:

- Low impact
- Medium impact
- High impact

POL.IMP.004: All IT Security incidents **shall** be categorised by the incident response team.

An IT incident may need to be recategorised if there are changes to the nature and impact of the incident.

Low impact incident

Low impact incidents are typically minor events such as a low-level breach in IT Security or a short-term loss of an IT service.

Medium impact incident

Medium impact incident are typically caused by:

- disregard for the MoJ IT Security Policy leading to a minor breach in security or the potential of data loss
- inappropriate use of MoJ IT assets
- theft or loss of data from an IT system that does not contain any personal information and is not protectively marked
- damage to an MoJ IT asset that impacts its usability
- connecting unauthorised equipment to an MoJ IT system
- prolonged or permanent failure of an MoJ IT system
- prolonged set of unsuccessful attempts to scan an IT network or instigate a denial of service attack
- a new critical security vulnerability in an IT system
- localised report of malicious code such as a virus on a terminal

High impact incident

High impact incidents require immediate escalation to the relevant Senior Information Risk Owner (SIRO), the MoJ Security Team, and the Data Protection Team if personal data is involved.

High impact incidents may require forensic investigation.

High impact incidents are typically caused by:

- malicious activity or espionage
- an incident that attracts media coverage
- intrusion into an IT network
- widespread malicious code attacks
- the theft or loss of personal or protectively marked data from an IT system

Escalations

If an incident needs to be escalated, it **shall** follow the chain of command through the incident response command structure.

The exact chain of escalation **should** be outlined in the IT system's Incident Response Plan.

A typical command chain might be from the incident manager to the Major Incident Management team, to the relevant SIRO to Chief Security Officer (CSO) to Ministerial response.

Reasons for escalation might include:

- issues of national security
- if the incident is receiving media coverage
- if the incident has caused harm to a member of staff or public
- the MoJ has suffered reputational damage
- a requirement to report to another Department or central management function
- significant actual or potential loss of personal information where the Information Commissioner’s Office and Cabinet Office need to be informed

POL.IMP.005: Each IT Security Incident Response Plan **shall** include a pre-arranged escalation path, where each stakeholder is named and is aware of their role. Contact the Major Incident Management team if you need help creating documented escalation paths.

Incident Management Stakeholders

There are likely to be both internal and external stakeholders involved in incident management and response.

These will vary depending on the specific IT system or service.

POL.IMP.006: All MoJ staff **shall** report any actual or suspected incidents, including breaches of MoJ Security Policy, to their line manager and to the IT Service Desk.

POL.IMP.007: As part of operational readiness, Each SIRO **shall** ensure that each IT system or service under their remit has an IT Security Incident Response Plan. A guide for writing a plan is available in the IT Security Response Plan and Process Guide.

POL.IMP.008: All High impact IT Security incidents and any IT Security incident involving personal data **shall** be reported to the SIRO for your business area.

POL.IMP.009: All IT Security incidents involving the suspected or actual loss, theft, or compromise of an Information Asset **shall** be reported to the Information Asset Owner (IAO).

POL.IMP.010: If the IT Service Desk receives a report of a security incident, this **shall** be reported to the MoJ Security Team.

Investigations

The MoJ Security Team is responsible for the investigation of all MoJ IT Security incidents.

If legal or disciplinary proceedings require evidence to be gathered, a forensic investigation may be needed.

POL.IMP.011: The MoJ Security Team **shall** maintain documentation on investigations undertaken.

POL.IMP.012: Any investigation of an IT Security incident and the events surrounding it **shall** be reported to all relevant stakeholders.

System Recovery

Following an IT Security incident, the IT system, services or any compromised assets **shall** be restored to business as usual (BAU).

If MoJ IT systems or services are restored using backups, the systems or services being restored **shall** pre-date the incident and **shall not** contain any weaknesses that could be exploited further.

POL.IMP.013: The IT Security Incident Response Plan **shall** show how an MoJ IT System or service will be restored or recovered following an IT Security incident. The method used to restore or recover an MoJ IT System **shall** be captured in the system's disaster recovery plan.

Lessons Learned

Once the cause of an IT Security incident has been identified steps **shall** be taken to make sure it will not happen again.

A report **shall** be prepared that describes:

- the incident
- the investigation
- the actions taken to restore the IT system or service to BAU
- all lessons learned

Lessons learned **should** include action points on how to improve the business systems to reduce the likelihood of the incident re-occurring.

This report **should** be sent to the SIRO who is responsible for forwarding it to all relevant stakeholders.

Information security aspects of business continuity management

Information security continuity

IT Disaster Recovery Plan and Process Guide

How to use this plan and process guide

This guide for technical users. Technical users include:

- Technical architects
- DevOps specialists
- IT service managers
- Software developers

This plan and process guide is part of a set of Ministry of Justice (MoJ) policies and supporting guides that cover various aspects of incident and disaster management and response.

The policies are:

- IT Security Incident Management Policy
- IT Disaster Recovery Policy
- IT Investigations - Planning and Operations Policy

The supporting guides are:

- IT Security Incident Response Plan and Process Guide
- IT Disaster Recovery Plan and Process Guide

This guide gives information on how to create and develop an IT Disaster Recovery Plan for your MoJ IT system or service.

The National Cyber Security Centre (NCSC) also offers guidance on how to effectively detect, respond to and resolve cyber incidents.

Business Impact Assessment

The service or system owner **should** carry out a Business Impact Assessment (BIA) in order to:

- get an overview of the Business as Usual (BAU) functions for the MoJ IT system or service
- get an understanding of the business criticality of the service the MoJ IT system supports
- calculate a Recovery Point Objective (RPO), this is the maximum amount of data the business can afford to lose during a disaster
- calculate a Recovery Time Objective (RTO), this is the amount of time before the disaster begins to seriously impede the flow of normal business operations

Suggested content

Disaster recovery plans are specific to each individual IT system or service. They are intended to offer guidance to every listed role when responding to an incident.

When deciding the content of a Disaster Recovery Plan for an MoJ IT system or service, a useful start is to identify every potential disaster that may affect the system or service, together with procedures to resolve each one.

Each Disaster Recovery Plan **should** include:

- the point at which the recovery plan **should** be used

- a clear and detailed process to recover the MoJ IT system to BAU
- a list of key roles and a description of their responsibilities - each role **should** have at least two sets of contact details
- a list of internal and external stakeholders to be contacted as soon as the incident happens, each stakeholder **should** have at least two sets of contact details
- a communication list of everyone who needs to be contacted, together with the chains of communication that **shall** be followed
- a list of people who can undertake the role of recovery manager
- a series of steps to follow in order to mitigate the incident
- a list of criteria needed to initiate a forensic investigation, and the role(s) responsible for it
- clear instructions on how to escalate to a higher level of incident response, to include names and contact details and the reason for escalating the incident
- methods to maintain business continuity whilst the MoJ IT service is unavailable
- a process to identify and capture lessons learned during the incident
- the requirement for a written report for medium and high impact incidents

All plans **should** be stored securely both online and offline. Roles and stakeholders mentioned in the plan **should** know of its location and be able to access it.

Reviewing and testing

Disaster Recovery Plans **shall** be reviewed regularly, and updated if there have been any changes to systems or services, personnel, or communication chains.

Plans **shall** be tested and practiced regularly to help familiarise each of the roles with their responsibilities within the response process.

This is not an exhaustive list. If you need support in creating a plan, please contact the Service Operations Centre (SOC) and the Major Incident Team.

Contact details

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

IT Disaster Recovery Policy

How to use this policy

This policy is for technical users. Technical users include:

- Technical architects
- DevOps specialists
- IT service managers
- Software developers

This policy is part of a set of Ministry of Justice (MoJ) policies and supporting guides that cover various aspects of incident and disaster management and response.

The policies are:

- IT Security Incident Management Policy
- IT Disaster Recovery Policy
- IT Investigations - Planning and Operations Policy

The supporting guides are:

- IT Security Incident Response Plan and Process Guide
- IT Disaster Recovery Plan and Process Guide

This policy describes what is needed to recover from an IT Disaster Event.

Information is listed beneath the following headings:

Policy Statements

This policy refers to Policy Statements, **POL.ITDR.001** to **POL.ITDR.014**.

POL.ITDR.XXX indicates the specific policy statement to be adhered to.

What is an IT disaster event?

An IT disaster event is any incident that causes actual or potential loss of availability or integrity of an MoJ IT system, which results in the MoJ IT system being unable to function during business as usual (BAU) operations.

What is IT disaster recovery?

IT disaster recovery is the planned response to a disaster event which will restore an IT system to BAU operations.

IT Disaster Recovery Plan

An IT Disaster Recovery Plan lists the actions to be taken to recover an IT system from a disaster event, together with a list of key roles and their responsibilities.

POL.ITDR.001: Each MoJ IT system **shall** have an IT Disaster Recovery Plan.

The IT Disaster Recovery Plan and Process Guide describes the information to include in a Disaster Recovery Plan.

Roles and Responsibilities

POL.ITDR.002: All Disaster Recovery Plans **shall** contain an up to date list of roles and responsibilities.

Each role **shall** have a name, with at least two sets of contact details.

POL.ITDR.003: All staff who are listed in a Disaster Recovery Plan **shall** be aware of their role and its responsibilities.

The list of roles and responsibilities **should** include internal and external stakeholders, together with everyone listed on the communications list.

The list of roles and responsibilities **shall** align with the Incident Management Plan (IMP).

A variety of individuals and teams may be responsible for business and IT service continuity, and escalation in case of a disaster. These may include:

- Executive Committee
- Senior Information Risk Owner (SIRO)
- Chief Security Officer (CSO)
- Information Asset Owner (IAO)
- Service Operations (SO), which includes the Major Incident Management Team and the Security Operations Centre (SOC)
- IT Service Continuity Management

A Disaster Recovery plan **should** include the relevant escalation process through the teams and individuals listed for each MoJ IT system.

Planning

An IT Disaster Recovery Plan supports the decisions and steps taken to reduce the effects of disasters and identifies the steps needed to recover MoJ IT systems back to BAU.

An IT Disaster Recovery Plan **shall**:

- contain identified risk scenarios and strategies to recover from them
- describe the circumstances in which the plan is invoked.

Business Impact Assessment

A Business Impact Assessment (BIA) **shall** be undertaken to identify the key disaster recovery requirements of the assets, services, and business processes supported by a specific MoJ IT system.

The BIA **should** contain:

- a Recovery Time Objective (RTO): the time between a disaster event occurring and full IT systems and services being restored
- a Recovery Point Objective (RPO): the period of time during which the business can tolerate data loss

POL.ITDR.004: A Disaster Recovery Plan **shall** contain an RTO and RPO. The plan may contain more than one of these depending on the system.

POL.ITDR.005: Any disaster recovery action **shall** ensure that the IT system can recover from a disaster within the RTO recorded in the BIA.

POL.ITDR.006: Any disaster recovery action **shall** ensure that the IT system can recover from a disaster within the RPO recorded in the BIA.

Testing and Readiness Review

An IT Disaster Recovery Plan **shall** be tested regularly to ensure that:

- the plan remains fit for purpose
- the plan reflects all changes in personnel and updates to system information
- everyone with a role in the plan knows their responsibilities

POL.ITDR.007: Each MoJ IT system **shall** have its IT Disaster Recovery Plan tested before commencing live operations.

POL.ITDR.008: All IT Disaster Recovery Plans **shall** be tested at least annually, and after significant update to an MoJ IT system. The testing schedule **shall** be outlined in the IT Disaster Recovery Plan.

POL.ITDR.009: The IT Disaster Recovery Plan **shall** be reviewed after each test and updated as required to ensure it is fit for purpose.

POL.ITDR.010: Each IT Disaster Recovery Plan **shall** define the circumstances when the plan is to be invoked.

Reporting and Alerting

The reporting and alerting structure of an IT Disaster Recovery Plan **should** align with that of the corresponding IT Security Incident Response Plan.

Every stakeholder that needs to be informed, **should** be listed as a key contact within the plan.

POL.ITDR.011: The reporting and alerting structure within an IT Disaster Recovery Plan **shall** align with the relevant IT Security Incident Management Plan and Business Continuity Plan. Responsibility for business continuity resides with the SO.

Recovery and Review

The process to recover from a disaster event **shall** ensure that security vulnerabilities are not introduced or re-introduced during the restoration process.

POL.ITDR.012: Each IT Disaster Recovery Plan **shall** contain pre-defined and tested processes and procedures to restore an MoJ IT system or services, which has been disrupted or disabled during a disaster event.

POL.ITDR.013: Each Disaster Recovery Plan **shall** describe in detail the procedures to enable an MoJ IT Security System return from recovery mode to BAU.

Lessons learned **shall** be collated in an after-action report and be fed back to appropriate stakeholders.

POL.ITDR.014: Following a disaster incident, an after-action report **shall** be produced, which contains:

- all lessons learned
- actions to be taken to update processes and plans

Contact details

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

IT Investigations - Planning and Operations Policy

How to use this policy

This policy is for technical users. Technical users include:

- Technical architects
- DevOps specialists
- IT service managers
- Software developers

This policy is part of a set of Ministry of Justice (MoJ) policies and supporting guides that cover various aspects of incident and disaster management and response.

The policies are:

- IT Security Incident Management Policy
- IT Disaster Recovery Policy
- IT Investigations - Planning and Operations Policy

The supporting guides are:

- IT Security Incident Response Plan and Process Guide
- IT Disaster Recovery Plan and Process Guide

Policy Statements

This policy refers to Policy Statements, **POL.POP.001** to **POL.POP.015**.

POL.POP.XXX indicates the specific policy statement to be adhered to.

IT Forensics

IT forensics is the collection, storage, analysis and preparation of digital evidence that might be required in legal or disciplinary proceedings,

Data used in a forensic investigation **shall** be collected, preserved and analysed using systemic, standardised and legally compliant methods.

This will ensure that data gathered is admissible as evidence in a legal case, dispute or disciplinary hearing relating to an IT security incident.

There are two types of forensic investigation:

- proactive forensic monitoring - as part of an indentified MoJ security control

- reactive investigation - where a suspicious incident has been identified or reported

A forensics investigation **should** be carried out:

- if an area needs proactive monitoring to enable forensic investigation
- if a business function makes a request via incident management escalation channels, to gather forensic evidence.
- if an investigation is requested as part of the IT security incident management process
- if requested as part of a leak investigation.

POL.POP.001: Each MoJ IT system or IT domain **shall** be covered by a Forensic Readiness Plan.

POL.POP.002: Each Forensic Readiness Plan **shall** include:

- an assessment of the risk management benefits
- authorisation from the IT Security Team and Senior Information Risk Officer (SIRO)
- a corresponding IT security incident management plan

Risk management benefits include risk assessments and cost-benefit-analysis, which will determine if an investigation is viable from a risk and cost perspective.

POL.POP.003: Forensic investigations in support of leak investigations **shall** be requested by the individual responsible for the leak investigation.

Integrity of Digital Evidence

POL.POP.004: Each forensic investigation **shall** be guided by the principles set out by the ACPO guidelines issued by the National Police Chiefs' Council (NPCC).

The integrity of data, which **might** subsequently relied upon in court, **shall** be maintained throughout the forensic investigation process.

Any person accessing data as part of an investigation **shall** be competent to do so and able to justify the relevance and implications of their actions.

Each investigation **shall** be documented clearly and leave an audit trail that will enable a third-party to examine each process and replicate the findings,

The person leading the investigation is responsible for ensuring that all methods used are carried out in accordance with the law.

Investigations **shall** be conducted in line with MoJ policies.

Evidence Collection and Storage

Security teams **should** be able to monitor systems to detect and respond to potential security incidents. If an incident needs to be investigated further, forensic tools **may** be used to assess and gather evidence.

The Forensic Investigation Owner (FIO) is responsible for the collection and management of digital evidence.

An external organisation **may** conduct the investigation on behalf of the MoJ.

Each item of evidence collected **shall** be managed according to the relevant Forensic Readiness Plan.

POL.POP.005: Each Forensic Readiness Plan **shall** include a process for the collection and storage of digital evidence, to include provision for where this task is conducted by an external organisation.

POL.POP.006: All users of an MoJ IT system **shall** be made aware that their access is monitored, and that IT forensic techniques **may** be used to capture evidence as part of an investigation into an IT security incident.

POL.POP.007: A Forensic Readiness Plan **shall** contain clearly defined procedures and methods for conducting a forensic investigation. The MoJ **shall** be able to resume business operations following an IT security incident. Any forensic investigation **shall** be conducted in a manner that enables the restoration of MoJ IT services.

POL.POP.008: A Forensic Readiness Plan **shall** consider business continuity arrangements to ensure that essential functions are able to be restored. Digital evidence **shall** be handled carefully in order for it to remain admissible.

POL.POP.009: Each forensic investigation **shall** have a clearly documented chain of custody for all digital evidence.

POL.POP.010: The MoJ Security Team is responsible for the integrity of digital evidence. Each forensic investigation **shall** have a named FIO who is responsible for the investigation and management of digital evidence.

POL.POP.011: Any investigative action taken on a piece of evidence **shall** be captured and recorded. This record **shall** include details of the action taken and the person responsible for undertaking that action.

POL.POP.012: Admissibility of evidence in a court of law depends on how the evidence was captured. Before capturing any evidence, advice **shall** be sought from the MoJ legal team and forensic investigation provider.

POL.POP.013: Each Forensic Readiness Plan **shall** include details of how to securely dispose of evidence when it is no longer required. This **shall** conform with Secure disposal of IT equipment.

Legal Requirements

Investigations of electronically stored information within the MoJ **shall** conform to the latest legal and regulatory guidelines.

BS 10008:2022 provides information on the collection of electronically stored information as evidence.

POL.POP.014: During each forensic investigation, methods used to capture digital evidence **shall** be in accordance with BS 10008:2022.

Reporting and Communication

Each IT Security Incident Management Plan contains a communication plan and an escalation plan that **shall** be followed when responding to an IT Security incident.

The IT Security Incident Response Plan and Process Guide gives more information.

For major incidents it might be necessary to consider escalating the forensic investigation process to an external body. This might be:

- Law Enforcement
- National Cyber Security Centre (NCSC)
- Cabinet Office
- MoJ legal advisors
- Other Government Agencies as required

POL.POP.015: Each Forensic Readiness Plan **shall** include the reporting structure and escalation path for internal and external teams and the individual responsible for managing the incident. This **shall** be consistent with the corresponding IT Security Incident Response Plan and Process Guidea. The forensic investigation process **shall** enable the chain of evidence to be passed to outside agencies, if required.

Contact details

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

IT Security Incident Response Plan and Process Guide

How to use this guide

This guide is for all users and is part of a set of Ministry of Justice (MoJ) policies and supporting guides that cover various aspects of incident and disaster management and response.

The policies are:

- IT Security Incident Management Policy
- IT Disaster Recovery Policy
- IT Investigations - Planning and Operations Policy

The supporting guides are:

- IT Incident Response Plan and Process Guide
- IT Disaster Recovery Plan and Process Guide

This guide gives information to help create and develop an IT Incident Response Plan for your MoJ IT system or service.

The National Cyber Security Centre (NCSC) also offers guidance on how to effectively detect, respond to and resolve cyber incidents.

Suggested content

Incident response plans are specific to each individual IT system or service.

When deciding what should go into an Incident Response Plan for an MoJ IT system or service, a useful start is to identify every potential incident that might affect the system or service, and list the ways to resolve each one.

Each Incident Response Plan **should** include:

- a list of key roles together with a description of their responsibilities - each role **should** have at least two sets of contact details
- a list of internal and external stakeholders to be contacted as soon as the incident happens, each stakeholder **should** have at least two sets of contact details
- a communication list of everyone who needs to be contacted, together with the chains of communication that **shall** be followed
- a list of people who can undertake the role of incident manager
- a series of steps to follow in order to mitigate the incident
- a method to identify the need for forensic investigation, and the role responsible for invoking it
- clear instructions on how to escalate to a higher level of incident response, to include names and contact details and the reason for escalating the incident
- a detailed process to recover the system to business as usual (BAU)
- a process to identify and capture lessons learned from the incident
- the requirement for a written report for medium and high impact incidents

All plans **should** be stored securely both online and offline. Roles and stakeholders mentioned in the plan **should** know of its location and be able to access it.

Incident response plans are intended to be flexible guides to help every role listed to respond to an incident.

Reviewing and testing

Incident Response Plans **shall** be reviewed regularly, and updated if there have been any changes to systems or services, personnel, or communication chains.

Plans **shall** be tested and practiced regularly to help familiarise each of the roles with the response process.

This is not an exhaustive list. If you would like support in creating a plan, please contact the Service Operations Centre (SOC) and the Major Incident Team.

Contact details

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

Compliance

Compliance with legal and contractual requirements

Data security and privacy

Data Security and Privacy

We believe that our technology must keep data safe and protect user privacy.

Our digital projects contain important information. Serious data breaches might result if we fail to:

- protect information
- handle it correctly at all times
- dispose of it safely when it is no longer required

Breaches might cause:

- harm to individuals
- financial loss to the Ministry of Justice (MoJ)
- a loss of confidence in us as an organisation

For personal data, the EU General Data Protection Regulation (GDPR) and UK Data Protection Act (2018) apply. These make the consequences of data breaches very clear.

To follow the data regulation/legislation, we **must** ensure that:

- we protect data to the best of our organisation's capabilities
- we collect data only for described, lawful purposes
- we use data only for the described, lawful purposes

Why are security and privacy important?

Breaches can have an adverse effect the relationship between citizen and government.

Not only do we have a duty to protect citizens data, but the penalties for violations are also severe. Under the GDPR, serious infringements can result in fines of up to €20M.

We must apply appropriate security and privacy protection to all the information we hold and process, at all times.

We should treat all data as sensitive unless proven otherwise.

All our work must follow this ethos.

When this applies

This principle applies to **all** MoJ technology projects and business activities.

While GDPR applies only to personal information, all MoJ projects and tasks must have excellent data security and privacy characteristics. If they handle personal data, they must do so correctly. Projects must follow MoJ guidelines unless exceptional and approved circumstances apply.

The Information Commissioner's Office (ICO) - the UK's independent regulatory office for data protection - has published guidance on how to determine what is personal data.

A Data Protection Impact Assessment (DPIA, formerly commonly known as a Privacy Impact Assessment or PIA) is required for all projects. There are some exceptions described by the ICO.

Data privacy

The MoJ Data Protection Team provides services, guidance, and support for all aspects of data privacy and protection.

For example, they have protocols and procedures to help ensure acceptable use of personal information.

Contact details

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

Risk Assessment Process

Risk Reviews

Information and the supporting processes, systems and networks are important and valuable Ministry of Justice (MoJ) assets. They are central to enabling the MoJ to perform its functions and provide services to the public, the legal professions, and other government departments and organisations.

Confidentiality, integrity and availability of information is essential to maintain the MoJ's ability to provide efficient and effective services, maintain compliance with legal and regulatory requirements, and maintain its and the Government's reputation.

The MoJ and its information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, sabotage, vandalism, fire and flood. Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated.

The MoJ's dependence on its information systems and services means that there is always a possibility of technology-enabled security threats. Connections between the MoJ's computer networks and public and other private networks, and sharing of information resources, further increase the difficulty of achieving and maintaining control.

It is essential that the MoJ identify its information security requirements. There are three main sources of these requirements.

- The legal, statutory, regulatory and contractual requirements that the MoJ, its partners, contractors and service providers have to satisfy.
- The principles, objectives and requirements for information processing that the MoJ and Government have developed to support their operations, for example the protective marking system and government baseline security standards.
- Assessed risks to the MoJ. Through risk assessment, threats to assets are identified, the potential business impacts of these threats are estimated, and the vulnerability to and likelihood of occurrence of the threats are evaluated.

Assessing information security risk

Security requirements are identified by a methodical assessment of security risks. Expenditure on security controls needs to be balanced against the business harm likely to result from security failures. Risk assessment is systematic consideration of:

- The business harm (the 'impact') which is likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets.
- The realistic likelihood of such a failure occurring in the light of the threats to and vulnerabilities of the system, and the controls currently implemented.

Managing information security risks

The results of the risk assessment are identified risks and risk severities. These help guide and determine the appropriate management action, and priorities for managing information security risks. Risks with a high severity level would justify the expenditure of more resources to control them than risks with a low severity level.
Risk Management involves identification, selection and implementation of justified security and contingency 'countermeasures' to reduce risks to an acceptable level.

Countermeasures can act in different ways such as:

- Reducing the likelihood of attacks or incidents occurring.
- Reducing the system's vulnerability.
- Reducing the impact of an attack or incident should it occur.

- Detecting the occurrence of attacks or incidents.
- Facilitating recovery from an attack or incident.

Risk management requires a judgement about what is an acceptable level of risk. Although this is a business decision, it does require a thorough understanding of the nature of the risk and the effectiveness of the countermeasures implemented to manage the risk. For some systems or scenarios, specialist advice might be needed.

When taking risk management decisions, consideration must be given to the full implications of the decisions taken. Failure to implement some countermeasures might breach legal or regulatory requirements. This is unlikely to be an acceptable risk management decision. Failure to meet other countermeasures might breach Government information security standards; as a consequence it might not be possible to link the MoJ system with other systems. This might limit the usefulness of the MoJ system.

Consideration must also be given to what are tolerable financial losses, political sensitivities and adverse publicity. The cumulative effect of accepting high levels of risk should also be taken into account.

Information security in projects

Information security controls are considerably cheaper and more effective if incorporated at the system requirements specification and design stage. Information risk assessments must be part of the project process.

Ongoing information security risk management

Effective risk management does not end once a risk assessment has been done and the required countermeasures implemented. Checks need to be carried out to ensure that the countermeasures are being applied effectively. It is also important to carry out periodic reviews of security risks and implemented controls to:

- Take account of changes to business requirements and priorities.
- Consider new threats and vulnerabilities.
- Confirm that controls remain effective and appropriate.

The role of security in risk assessment and risk management

The MoJ security team can provide help in all areas of security risk management for systems. Examples include:

- Advice on risk assessments.
- Help with carrying out risk assessments.
- Assist with the risk management decision process.
- Help with creating and managing documentation compliant with MoJ standards.
- Assisting with mandatory Government risk assessments.
- Advice on compliance checking.

Contact details

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

Glossary and Acronyms

Glossary

This information is a reference list of Ministry of Justice (MoJ) terms and abbreviations.

A more extensive list of acronyms is available here.

The NCSC has a comprehensive cybersecurity glossary available on its website.

Terms

2FA	Refer to Multi-factor authentication.
Authorised User	Any user of services covered as authorised by the MoJ.
Blue Team	The internal security defence team in an organisation. Within the MoJ, this work is performed by the Security Team.
Brute Force Attack	The application of lots of computer power, to try and perform a task using a huge number of values. Typically used to try out many passwords, to gain access to systems.
Business Continuity Plan (BCP)	A document that outlines the procedures in place for a business to continue to operate, despite an unexpected disruption to services. These disruptions might be things such as cyber attacks, pandemics, or natural disasters.
Credentials	Information used to prove someone's identity, to confirm that they really are who they say they are. Typically includes passwords, tokens, and certificates.
Critical infrastructure attack	Critical infrastructure refers to the physical and cyber structures, facilities, and systems that are essential for a country to function. Attacks on these resources would harm the physical security, economic security, or public health of the country.
Customer	Someone who buys goods or services. The customer of an IT service provider is the person or group who defines and agrees the service level targets. The term customers is also sometimes informally used to mean users, for example "this is a customer focused organisation".
Dark web	Generic name for encrypted online content that is not indexed by search engines. The information is only accessible with special software or tools.
Data breach	An incident where data is accessed in a non-authorised way.
Decryption	The reverse of an encryption process.
Distributed Denial of Service (DDoS) attack	Legitimate users cannot access computer services, because threat actors are overloading the service with requests. Also referred to as a Denial of Service (DoS) attack.
Digital footprint	A collection of data and information traces left behind by a user, as they do activities online. For example, all the things you've ever searched for on Google.
Double encryption ransomware	Refer to ransomware.
Encryption	The process of converting human-readable text into unreadable 'disguised' information, or 'ciphertext'. You can see it, but you can't understand it. Only someone with a decryption key can convert ('decrypt') the unreadable information back into human-readable form again.

Exfiltrate	The formal name for a technique used by threat actors and malware to surreptitiously copy and transfer data out of a system. This is data theft.
Exploit	A program or process that takes advantage of a vulnerability in a system to cause system problems, or to access or modify information without authorisation.
Incident	Any event which is not part of the standard operation of a service, and which causes, or might cause, an interruption to, or a reduction in, the quality of that service. A breach of the security rules for a system or service.
Incident Management	The process responsible for managing the lifecycle of all incidents. The primary objective of incident management is to return the IT service to users as quickly as possible.
Insider threat	Any threat from current or former employees of an organisation who have inside information or authorised credentials that might be used to cause harm to the organisation, accidentally or maliciously.
Macro	A small program or script that automates tasks in an application, such as Microsoft Office. Might be used by attackers can use to gain access to, or harm, a system.
Malware	Malicious software. This includes things like viruses, trojans, worms, or any code that can have a negative impact on an a system.
Multi-factor authentication (MFA)	Use of two or more different components to verify a user's claimed identity. Typically an extra component, in addition to a password. MFA often uses an authenticator app or SMS text to deliver a single use code. Also Two-factor authentication (2FA).
Open Source Intelligence (OSINT)	Information gathered from public information. This includes data from social network accounts, company websites, and other openly available information sources.
Operational Security Team (OST)	Deprecated name for the Security Team within the MoJ. The Security Team help protect against cyber attacks, and help manage incidents. Sometimes referred to as the Blue Team. They can be contacted through email: security@justice.gov.uk.
Out of band check	An additional check performed using a different communication channel, to verify identity or intent. The check helps prevent phishing or social engineering attacks. For example, if you receive an email from a senior manager, asking you to perform an unusual task, you should want to check that the request is genuine. If you reply by email to the original request, that's an 'in band' check, and can't be trusted, because it's possible the manager's email has been compromised. But if you called the manager by mobile phone to check the request, that's using a different communication technology, so it's an out of band check. A threat actor would have to compromise both the manager's email and their mobile phone account to succeed in tricking you. For more

	detail on out of band checks, refer to this additional information.
Password	A secret string of characters, numbers, and often symbols. When used with a valid user ID, a password enables access to an account.
Patching	Applying updates to software or firmware to improve security and enhance functionality.
Phishing	Untargeted mass emails sent to many individuals. The email typically asks for sensitive information, or encourages you to visit fake websites, or to send money. For more information, refer to the phishing guide.
Problem	A cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the Problem Management process is responsible for further investigation.
Problem Management	The process responsible for managing the lifecycle of all problems. The primary objectives of Problem Management are to prevent incidents from happening, and to minimise the impact of incidents which cannot be prevented.
Process	A structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process might include any of the roles, responsibilities, tools, and management controls required to deliver the outputs reliably. A process might define policies, standards, guidelines, activities, and work instructions if they are needed.
Ransomware	Malicious software that makes data or systems unusable by encrypting it and then demanding a payment from the victim to decrypt it. Double Extortion Ransomware exfiltrates the data before encryption and demands a ransom payment to stop the threat actor releasing the data to the public, as well as for decrypting the system.
Red team	This is an internal or external team that tests organisational security by simulating cyber attacks as realistically as possible. Together with the Blue Team, the team helps to improve the cyber defences of the organisation.
Resolution	Action taken to repair the fundamental cause of an incident or problem, or to implement a workaround.
Resolver Group	May include a wide range of IT teams, including support and development personnel, other Service Management Functions (SMFs), other units within the organisation, outsourcing providers, partners, and other third parties.
Service Desk	The single point of contact between the service provider and the users. A typical Service Desk manages incidents and service requests, and handles communication with the users.

Social engineering	Manipulating people into doing things or divulging information that is of use to a threat actor.
Tabletop	An exercise created to try out Business Continuity Plans (BCPs). These exercises create realistic scenarios, and play through a number of obstacles, to ensure organisations have robust BCPs.
Tailgating	An unauthorised individual forcefully or stealthily gaining access to a building, typically by entering immediately behind an authorised user.
Threat actor	A general term that encompasses all types of individuals and groups that use cyber methods to cause harm. This includes competitors seeking to steal information, cyber criminals attacking for political or monetary gain, accidental or malicious insider threats, spies, social and political activists, and assorted hackers.
Trend Analysis	Analysis of data to identify time related patterns. Trend analysis is used in Problem Management to identify common failures or fragile configuration items, and in Capacity Management as a modelling tool to predict future behaviour. It is also used as a management tool for identifying deficiencies in IT Service Management Processes.
Virtual Private Network (VPN)	An encrypted network created to allow secure connections for remote users.
Vulnerability	A weakness in software, a system, or process. A threat actor might seek to exploit a vulnerability to gain unauthorised access to a system.
Zero day (0day)	A vulnerability in a system that few people know about. threat actors can exploit an 0day to attack or affect data and systems.
Zero trust	The assumption that all requests and connections are potential breaches, and so must be verified and authenticated before being allowed.

Out of band checks

An out of band check is when an individual uses a different method of communication than the one the message came from. This method means that if one communication method is compromised, you quickly find out by using a different communication method to confirm validity. The likelihood of multiple communication methods for the same person or team being compromised is low.

Out of band checks are an easy method to confirm the legitimacy of communications and requests. They can confirm the identity behind a message or request, and they can confirm the validity of the message or request itself. Social engineering techniques and phishing tactics take advantage of people who do not use out of band checks. By doing an out of band check, these sorts of attacks can be stopped very easily.

Example 1: You receive an email request for an urgent review of an invoice, and immediate payment. The email comes from someone unexpected. You should find the official contact details of that person, and contact them using a phone call - but not email - to confirm that they did indeed send the original email. If they did send the email, you can proceed with the request. If they did not send the email, you can report the email as a phish, and also alert the owner of the email address that their email address might have been compromised.

Example 2: You receive a phone call from someone claiming to be your bank, or HMRC, or HMCTS. You hang up the call, and locate the official website for the company. You should be able to find multiple official contact details there. Use one of these to contact the place the caller claimed to be from. If, for example, the claim was that your bank was calling, you can call the direct number and speak to the switchboard about the reason for the initial call. They will forward you to the correct department. You can then confirm the validity of the original call, and so confirm whether the original caller was actually from your bank or not.

Example 3: Someone enters your place of work, and claims to have a meeting with a specific person. Unfortunately, there is no record of this on the expected visitor list. You can call or email the person within your place of work to confirm the visitor is legitimate. This check also works if tradespeople arrive unexpectedly, because you can contact both the relevant person within your place of work and also contact the company they claim to be from, using the company's official website contact details.

Example 4: You receive an email requesting that you reset your password immediately. The email contains a link to perform the password reset. You have not attempted to login to that account recently. You should use an internet search for the website or type the URL directly if you know exactly what it should be. When you attempt to login, the website will let you know if you need to reset your password. If not, you know someone else has attempted to gain access to your account. That would mean the password reset request was not legitimate, and most likely a phishing attempt hoping to get your username and password through the reset link in the original email. Similarly, if you get an MFA request unexpectedly, do not confirm it unless you were indeed attempting to access that account immediately before the request came through. If you get an MFA request, but had not been trying to connect using the account, you should change the account password as soon as possible, because it might have been compromised.

When doing an out of band check, be sure to pick a different method of communication to the one used to contact you originally. If someone emails you unexpectedly, perform an out of band check by making a phone call. If someone calls you, perform an out of band check by using the Internet. It is very unlikely that multiple communication channels have been compromised.

Be sure to get official contact details for companies only from their official websites. Never be afraid to hang up on someone and check their identity through another method, especially if they are asking for sensitive or personal information or credentials. Never be afraid to check the legitimacy of unusual email requests. by contacting the sender through a different communication channel.

Doing an out of band check lets you confirm that the messages come from the person they claim to be, and that the requests are valid. This helps prevent you or your company from losing money to fake invoices, from accidentally giving up sensitive information or credentials, and from having unauthorised individuals in your place of work. Doing an out of band check is fast and easy.

All members of your workplace should be happy to receive such a check. It shows that you take security seriously, and that you are helping to protect them as well as yourself.

Contact details

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