



Ministry
of Justice

Cyber Security Guidance

General Edition



Contents

Cyber and Technical Security Guidance.....	6
Summary.....	6
Change log.....	6
Offline content.....	6
Searching this content.....	6
Security culture.....	6
Getting in touch.....	6
Information structure.....	7
Information security policies.....	7
Mobile devices and teleworking.....	7
Human resource security.....	7
Asset management.....	8
Access control.....	8
Physical and environmental security.....	9
Operations security.....	9
Communications security.....	9
Information security incident management.....	10
Compliance.....	10
Risk Assessment.....	10
Other Guidance.....	10
Glossary.....	10
Acronyms.....	10
Technical Guidance.....	10
Feedback.....	10
 Change log for Ministry of Justice (MoJ) Security Guidance.....	 10
 Getting in contact.....	 14
Reporting an incident.....	14
Security Team: asking for help.....	14
Overview.....	14
About the team.....	14
Asking for help.....	14
How the team handle requests for help.....	15
What happens next.....	15
If things go wrong.....	15
 Security culture.....	 15
Security culture.....	15
Who is this for?.....	15
Christmas SMS delivery scams.....	15
Contact details.....	16
 Information security policies.....	 16
Management direction for information security.....	16

Avoiding too much security.....	16
IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER.....	16
IT Security Policy (Overview).....	17
Line Manager approval.....	22

Mobile devices and teleworking..... 23

Mobile device policy.....	23
Mobile Device and Remote Working Policy.....	23
Teleworking.....	29
Accessing MoJ IT systems from overseas.....	29
General advice on taking equipment overseas.....	32
Overseas travel.....	34
Personal devices.....	35

Human resource security..... 36

Prior to employment.....	36
Minimum User Clearance Requirements Guide.....	36
National Security Vetting for External Candidates FAQ.....	37
National Security Vetting contact.....	40
National Security Vetting questions.....	41
Pre-employment screening.....	45
Pre-Employment Screening and Vetting of External Candidates - FAQs.....	45
Security clearance appeals policy.....	49
Security clearance appeals procedures.....	50
Security vetting assessment of need.....	55
During employment.....	55
Ongoing Personnel Security.....	55
Personnel risk assessment.....	57
Reporting personal circumstance changes.....	59
Training and Education.....	61
Voluntary drug testing policy.....	61
Voluntary drug testing policy procedures.....	62
Termination and change of employment.....	65
End or change of employment.....	65
Leavers with NSC and NSVCs.....	65

Asset management..... 66

Responsibility for assets.....	66
Acceptable use of Information Technology at work.....	66
Acceptable Use Policy.....	69
Guidance on IT Accounts and Assets for Long Term Leave.....	74
Protect yourself online.....	75
Information classification.....	76
Data Handling and Information Sharing Guide.....	76
Government Classification Scheme.....	81
Information classification, handling and security guide.....	85
Media handling.....	94
Removable media.....	94
Secure disposal of IT equipment.....	95
Working securely with paper documents and files.....	98

Access control..... 101

User responsibilities.....	101
Protecting social media accounts.....	101
System and application access control.....	104
Password Managers.....	104
Passwords.....	105
Using LastPass Enterprise.....	109
Physical and environmental security.....	110
Secure areas.....	110
CCTV policy.....	110
Entry and exit search policy.....	111
Personal mail and parcel delivery policy and procedure.....	111
Physical Security Policy.....	113
Public protest and demonstrations policy.....	115
Security in the office.....	117
Security threat level and emergency procedures.....	118
Visitor Access Policy.....	119
Equipment.....	125
Clear screen and desk.....	125
Equipment Reassignment Guide.....	126
Laptops.....	127
Locking and shutdown.....	128
Policies for MacBook Users.....	130
Operations security.....	131
Protection from malware.....	131
Ransomware.....	131
Control of operational software.....	132
Guidance for using Open Internet Tools.....	132
Communications security.....	135
Information transfer.....	135
Bluetooth.....	135
Email.....	138
General app guidance.....	144
Phishing Guide.....	149
Secure Data Transfer Guide.....	153
Sending information securely.....	156
Web Browsing.....	160
Wifi security policy.....	163
Information security incident management.....	166
Management of information security incidents and improvements.....	166
Lost devices or other IT security incidents.....	166
Compliance.....	167
Compliance with legal and contractual requirements.....	167
Data security and privacy.....	167
Risk Assessment Process.....	168
Risk Reviews.....	168
Assessing information security risk.....	169

Managing information security risks.....	169
Information security in projects.....	169
Ongoing information security risk management.....	169
The role of security in risk assessment and risk management.....	170
Contact details.....	170

Glossary and Acronyms..... 170

Glossary.....	170
Terms.....	170
Out of band checks.....	174
Contact details.....	175

Cyber and Technical Security Guidance

Summary

This site documents some of the security decisions that the [Ministry of Justice \(MoJ\)](#) has made for the products we operate, and our relationships with suppliers.

The MoJ [Technical Guidance](#) covers technical decisions in the MoJ more widely.

Note: This guidance is dated: 19 April 2022.

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.

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 19 May 2022. For the latest, current version of the guidance, refer to the [security guidance site](#).

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.

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 is 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 [here](#).

Getting in touch

- [To report an incident](#).
- For general assistance on MoJ security matters, email security@justice.gov.uk.
- For Cyber Security assistance or consulting, email security@justice.gov.uk. More information about the Security Team is [available](#).
- Suppliers to the MoJ should first communicate with their usual MoJ points of contact.

Information structure

The documents are listed in the next section.

Information security policies

Management direction for information security

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

Mobile devices and teleworking

Mobile device policy

Mobile Device and Remote Working Policy	All users (Policy)
Remote Working	All users

Teleworking

Accessing MoJ IT systems from overseas	All users
General advice on taking equipment overseas	All users
Personal Devices	All users

Human resource security

Prior to employment

Minimum User Clearance Levels Guide	All users
National Security Vetting contact	All users
National Security Vetting questions	All users
National Security Vetting for External Candidates FAQ	All users
Pre-employment screening	All users
Pre-Employment Screening and Vetting of External Candidates - FAQs	All users
Security clearance appeals policy	All users
Security clearance appeals procedures	All users
Security vetting assessment of need	All users

During employment

Ongoing Personnel Security	All users
Personnel risk assessment	All users

Reporting personal circumstance changes	All users
Training and Education	All users
Voluntary drug testing policy	All users
Voluntary drug testing policy procedures	All users

Termination and change of employment

End or change of employment	All users
Leavers with NSC and NSVCs	All users

Asset management

Responsibility for assets

Acceptable use	All users
Acceptable use policy	All users (Policy)
Guidance on IT Accounts and Assets for Long Term Leave	All users
Protect Yourself Online	All users
Web browsing security	All users

Information classification

Government Classification Scheme	All users
Information Classification and Handling Guide	All users
Information Classification and Handling Policy	All users (Policy)

Media handling

Removable media	All users
Secure disposal of IT equipment	All users
Secure disposal of IT - physical and on-premise	All users
Working securely with paper documents and files	All users

Access control

User access management

User responsibilities

Protecting Social Media Accounts	All users
--	-----------

System and application access control

Password Managers	All users
Passwords	All users
Using LastPass Enterprise	All users

Physical and environmental security

Secure areas

CCTV policy	All users
Entry and exit search policy	All users
Personal mail and parcel delivery policy and procedure	All users
Physical security policy	All users
Public protest and demonstrations policy	All users
Security in the office	All users
Security threat level and emergency procedures	All users
Visitor access policy	All users

Equipment

Clear Screen and Desk Policy	All users
Equipment Reassignment Guide	All users
Laptops	All users
Locking and shutdown	All users
Policies for MacBook Users	All users

Operations security

Protection from malware

Ransomware	All users
----------------------------	-----------

Control of operational software

Guidance for using Open Internet Tools	All users
--	-----------

Communications security

Information transfer

Bluetooth	All users
Email	All users
General Apps Guidance	All users
Phishing Guide	All users
Secure Data Transfer Guide	All users
Sending information securely	All users
Web browsing security policy profiles	All users (Policy)
Wifi security policy	All users (Policy)

Information security incident management

Management of information security incidents and lost devices

Lost devices or other IT security incidents	All users
Reporting an incident	All users

Compliance

Compliance with legal and contractual requirements

Data Security and Privacy	All users
---	-----------

Risk Assessment

Risk Assessment Process

Risk reviews	All users
------------------------------	-----------

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.

2022-04-19 17:45 BST [Update links for contacting security team.](#)

Standardise on security@justice.gov.uk email address for contacting security team.

2022-04-08 10:09 BST [Add guidance on secure disposal of cloud materials.](#)

New guidance to ensure the confidentiality of MoJ data remains when a cloud service is decommissioned.

2022-04-06 15:53 BST Update security.txt link.	Corrected link to the standard security.txt file.
2022-04-04 10:50 BST Add password manager guidance.	Added extra information on the use of password manager apps in the MoJ.
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.
2022-01-18 09:13 GMT Updated Overseas Travel Form	Updated Overseas Travel Form.
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.
2021-12-13 11:27 GMT Debrief on return from travel	Added description of a security debrief that is mandatory after some travel or where other security conditions apply.
2021-12-13 11:24 GMT Accessing MoJ systems from overseas	Added link to supplementary information on the MoJ Intranet.
2021-12-08 09:15 GMT Email access	Added clarification regarding when access is permitted to a user's business email account.
2021-12-07 15:18 GMT Email Authentication	Added guidance requiring the use of MTA-SLS and TLS-RPT in MoJ email systems.
2021-12-03 13:39 GMT Visitor Access Policy	Policy regarding the access and security management controls that are in place for all visitors to MoJ buildings.
2021-12-02 16:54 GMT National Security Vetting Contact	Updated application form for candidacy to be an NSVC.
2021-11-30 13:54 GMT Personal Devices	Clarified guidance on connecting personal devices using Bluetooth, and added new section on connected vehicles.
2021-11-22 16:23 GMT MFA	Clarified guidance on sending one-time MFA codes only to individual devices or accounts, not to shared devices or accounts.
2021-11-22 14:14 GMT Government Classification Scheme	Updated and consolidated guidance on classification of Government information.
2021-11-19 15:22 GMT Other guidance and security.txt	Improved structure for other guidance information, and added security.txt file.
2021-11-19 14:29 GMT Security in the office	Key security points for working in a Ministry of Justice location.
2021-11-19 10:09 GMT Sending information securely	Guidance on working securely with paper documents and files.
2021-11-18 17:03 GMT Protests and demonstrations	Policy and guidance on public protests and demonstrations.
2021-11-17 17:07 GMT Personal devices	Updated guidance about using a personal device to connect to a business Teams meeting as a Guest.
2021-11-09 15:37 GMT Acceptable use policy	Provide more detail on monitoring of systems and information, and to clarify the situation regarding Data Protection and the storage or processing of information outside the UK.
2021-11-08 17:30 GMT System backup policy	Corrected broken links within the content, also some structural changes for easier cross-referencing with related topics.
2021-11-04 10:28 GMT CCTV Policy	This policy details the purpose, usage, and management of the CCTV systems within the MoJ.
2021-11-04 09:05 GMT Working securely with paper documents and files	This guidance helps you understand the risks involved in working with, sharing, and moving paper documents both inside and outside the office.

2021-11-03 17:12 GMT Email blocking	The policy and processes for blocking emails, and deleting emails through administrative processes, across email services across the MoJ.
2021-11-03 17:00 GMT Domain names	An overview of domain name registration and monitoring principles and responsibilities within the MoJ.
2021-10-29 11:52 BST Logging retention	Information about keeping logging information.
2021-10-20 09:53 BST National Security Vetting contacts	Updates to the process and information for National Security Vetting contacts.
2021-10-19 13:06 BST Remote working	Simplified the guidance regarding remote working.
2021-10-15 16:27 BST Email best practices	Added guidance regarding attachments and the use of 'cc' and 'bcc' fields in emails.
2021-10-15 13:39 BST Security clearance appeals procedures	Added guidance for appealing a security clearance decision.
2021-10-14 13:47 BST Azure subscription baselines	Added guidance on baselines and templates for Azure subscriptions.
2021-10-13 15:50 BST IT Health Checks	Added guidance on requesting and managing IT Health Checks.
2021-10-13 09:26 BST User clearance requirements	Clarification to minimum user clearance requirements.
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.
2021-09-06 09:21 BST National Security Vetting contacts.	Information on the role and registration process.
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.
2021-08-17 09:26:00 BST Provide offline version of Group Security content.	Created PDF and eBook versions of the security policy and guidance subset for Group Security.
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. Alternatively, if the incident is of a cyber security nature then use [Report a cyber security incident](#).

Related information

[Security in the office](#) on page 117

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 privacy@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.

This poster shows you examples of typical scam SMS messages. It explains what FluBot is and how to remove it. It tells you about the best practices for avoiding being a victim of these scams.

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.

The leaflet is available [here](#).

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.

Remember also that within the MoJ, systems almost always have [RFC1918](#) addresses. These are normally not routable from the Internet. If you can access the system from the Internet, then you have other problems to resolve. Address them by appropriate security measures rather than hoping that secrecy is enough.

In other words, avoid saying that 'all IP addresses and domain names must be secure'. Instead, think about and justify the handling protections around each piece of information. Ask what data or capability is actually in need of protection, and from what risks.

It's not only about domain names or IP addresses

The need to keep some aspect of a system secret might be evidence that the technical security measures around the system are not complete, adequate, or appropriate to the risks. A well-designed system won't depend on secrecy alone for security.

IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

The Ministry of Justice (MoJ) is required to adhere (but prefers to exceed) to the [Minimum Cyber Security Standard \(MCSS\)](#).

The Standard

The [UK HMG Security Policy Framework](#) mandates protective security outcomes that the MoJ must achieve (and suppliers to MoJ, where they process MoJ data/information).

More information is available from <https://www.gov.uk/government/publications/the-minimum-cyber-security-standard>.

IDENTIFY

IDENTIFY is a prerequisite standard that requires:

- appropriate information security governance processes;
- identification and cataloguing of information held/processed; and
- identification and cataloguing of key operational services provided.

PROTECT

PROTECT is the core standard to provide fundamentally defences to information and requires:

- access to systems and information to be limited to identified, authenticated and authorised systems/users;
- systems to be proportionally protected against exploitation of known vulnerabilities; and
- highly privileged accounts (such as administrative level) to be protected from common attacks.

DETECT

DETECT is the core standard to detect when attacks are taking, or have taken, place and requires:

- capture event information (and apply common threat intelligence sources, such as [CiSP](#));
- based on PROTECT, define and direct monitoring tactics to detect when defence measures seem to have failed;
- detection of common attack techniques (such as commonly known applications or tooling); and
- implementation of transaction monitoring solutions where systems could be vulnerable to fraud attempts.

RESPOND

RESPOND is the core standard to define the minimum of how organisations should respond to attacks and requires:

- development and maintenance of an incident response & management plan (including reporting, roles and responsibilities);
- development and maintenance of communication plans, particularly to relevant supervisory bodies, law enforcement and responsible organisations such as the NCSC;
- regular testing of the incident response & management plan;
- assessment and implementation of mitigating measures on discovery of an incident (successful attack); and
- post-incident reviews to ensure feedback into the iteration of the incident response & management plan.

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 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 **MUST** 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 MoJGroup Security (mojgroupsecurity@justice.gov.uk) 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 [Accessing MoJ IT Systems From Overseas](#) information.

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.	<p>Implementing and managing information risk management in their respective business groups.</p> <p>Regularly reviewing the application of policy and guidance to ensure it remains appropriate to their business objectives and risk environment.</p> <p>Authorising any exceptions and deviations from the IT Security Policy with consideration of the impact any changes might have to other users.</p>
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, also known as IA Leads, 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.	<p>Logging and monitoring.</p> <p>Reviewing access permissions.</p> <p>Understanding and addressing risks associated to their information assets.</p> <p>Ensuring secure disposal of information when it is no longer required.</p>
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.	<p>Verify that contracts are written to reflect the MoJ's IT Security Policy.</p> <p>Ensure contractors comply with the requirements set out by this policy and associated documentation.</p>

Role	Responsibility	Which includes...
		<p>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.</p> <p>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.</p>

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.

Examples include:

- [General advice on taking equipment overseas](#).
- [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

Related information

[Security in the office](#) on page 117

Introduction

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

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

Audience

This policy is aimed at:

Technical users

These are in-house MoJ Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the

	Event, Problem, Incident, CSI, and Knowledge (EPICK) Team.
Service Providers	Any other MoJ business group, agency, contractor, IT supplier, and partner who in any way designs, develops or supplies services, including processing, transmitting, and storing data for, or on behalf of, the MoJ.
General users	All other staff working for the MoJ

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

Mobile devices

POLMOB001 : When using mobile devices, special care **SHALL** be taken to ensure that business information is not compromised. When issuing or using MoJ mobile devices, the following points **SHALL** be adhered to:

- POLMOB002 : Mobile devices **SHALL** be registered as an MoJ asset.
- POLMOB003 : Software installation **SHALL NOT** be available for general users, except when using an approved MoJ process or tool, such as an MoJ self-service app store.
- POLMOB004 : There **SHALL** be an ability for remote disabling, erasure or lockout.
- POLMOB005 : **ONLY** MoJ approved web services and web apps **MAY** be used.

Use in public places

POLMOB006 : Care **SHALL** be taken when using mobile devices in public places, meeting rooms, and other unprotected areas. Protection **SHALL** be in place to avoid the unauthorised access to, or disclosure of, the information stored and processed by these devices.

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

Theft or loss

POLMOB007 : Mobile devices **SHALL** be physically protected against theft, especially when left unattended. Examples include leaving devices unattended in cars and other forms of transport, hotel rooms, conference centres, and meeting places.

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

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

Use of private equipment

POLMOB009 : You **SHOULD NOT** use personal devices for MoJ work purposes.

Exceptions are possible on a case-by-case basis, for example to accommodate Accessibility requirements. To discuss whether you have a case for exemption, [contact the 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.

POLMOB010 : The MoJ allows remote working, but the following points **SHALL** be considered, confirmed, and documented as acceptable during the approval process:

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

POLMOB011 : The guidelines and arrangements for remote working **SHOULD** be considered, including:

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

Current supporting documentation:

- [Remote Working](#)
- [Accessing MoJ IT Systems from Overseas](#)
- [Security Guidance for Using a Personal Device](#)
- [General advice on taking equipment overseas](#)

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 Related information

[Security in the office](#) on page 117

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:** Avoid using [Hotel or other public wifi spots](#). They are not secure and can potentially monitor your equipment and information. Instead, you should use an MoJ-provided mobile data (4G) connection.
- **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 eg 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.

For these reasons:

- **Do:** Avoid using public wifi or internet services for MoJ business.
- **Do:** Avoid connecting MoJ equipment to public wifi or internet services.

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

- Tel: 0800 917 5148
- [MoJ Service Portal](#)

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

Privacy Team

- Email: privacy@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

Accessing MoJ IT systems from overseas

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

Note: If you are national security cleared to SC or DV levels, or subject to STRAP briefing, follow this process for all your trips, regardless of whether they are for business or personal reasons.

As a government official travelling overseas, you should consider that you may be of interest to hostile parties regardless of your role. By following MoJ policies and processes, you can help reduce the risk to yourself and limit the damage of exposure of sensitive information.

Essential guidance is provided in the [overseas travel information](#).

In general, it is acceptable for MoJ users to access MoJ services from overseas, and to do this using their MoJ equipment. But before you travel, consider:

- Do you need to take MoJ IT equipment overseas or access MoJ IT systems to do your job?
- Can the business need be met in another way or by someone else?

- If you just need to manage your inbox while away, can you delegate permissions to your inbox to a colleague to manage on your behalf?
- Have you left enough time to check and obtain necessary approvals? The process can take several weeks, depending on the circumstances. This is because it may be necessary to apply additional technical controls to protect you, your devices, and any data the devices can access.

Steps to follow before travelling

Part One

1. Get confirmation from your Senior Line Manager (Head of your immediate team) that there is a business need for you to take MoJ IT equipment overseas and access MoJ services. Keep a note of the answers you get.
2. Your Senior Line Manager **SHOULD** inform your HR Business Partner (HRBP) of your request to work overseas. The HRBP **SHALL** advise your Senior Line Manager of any HR considerations concerning your request.
3. If you are subject to STRAP briefing and intend to travel to or through any country not in Western Europe, North America, Australia, or New Zealand, then you **SHALL** notify the STRAP team at STRAPTeam@cluster2security.gov.uk and proceed directly to **Part Two** of this process.
4. Proceed directly to **Part Two** of this process if you are travelling to or passing through one of the following countries:

Argentina, Armenia, Azerbaijan, Belarus, China (including Hong Kong, Macau, and Tibet), Cuba, Egypt, Estonia, France, Georgia, Germany, India, Indonesia, Iran, Iraq, Israel (including Palestinian territories), Kazakhstan, Kyrgyzstan, Latvia, Lebanon, Libya, Lithuania, Moldova, the northern area of the Republic of Cyprus, North Korea, Pakistan, Russia, Saudi Arabia, Serbia, South Africa, South Korea, Syria, Taiwan, Tajikistan, Turkey, Turkmenistan, UAE, Ukraine, Uzbekistan, Vietnam.
5. If you have reached this step, you do not need to seek further formal approval for your trip.
6. **Take a copy of this guidance**; it includes useful contact details that help in the event of a problem while travelling.
7. Check if you need to do anything to prepare for **International Roaming**. Refer to the **International Roaming** section.

Part Two

1. Collect the following information:
 - Name.
 - Email address.
 - Your business area.
 - Your Security Clearance.
 - The network you use to access MoJ data, services, or applications, for example DOM1 or Quantum/MoJO, or online services such as AWS or Google Workspace.
 - The make/type of equipment you want to take with you.
 - Asset Tag details.
 - Countries you'll be visiting or passing through.
 - Dates of travel.
 - Transport details where possible, for example flights or rail journeys.
 - Proposed methods of connecting to MoJ systems or services, for example MoJ VPN, Global Protect VPN (for Macs), wifi, or Mobile Data (3G/4G/5G).
 - Reason for maintaining access while overseas.
 - The MoJ data, applications, or services you expect to access during your trip.
 - Who you are travelling with.
2. The next step depends on your MoJ business area:
 - If you are part of MoJ HQ, HMPPS HQ, HMCTS, or NPS, contact your Senior Line Manager and ask for approval to take MoJ equipment overseas and access MoJ services. Ask for any special details or considerations that apply to your proposed travel arrangements. Keep a note of the answers you get.

- If you are part of HMPPS (but *not* HQ), contact your Governor and ask for approval to take MoJ equipment overseas and access MoJ services. Ask for any special details or considerations that apply to your proposed travel arrangements. Keep a note of the answers you get.
3. Fill in the [overseas travel form](#).
 4. Send the completed form to security@justice.gov.uk, including the answers obtained from the earlier parts of this process.
 5. Your request will be considered, and an answer provided, as quickly as possible.
 6. When you receive approval for your trip, you might need to schedule a [debrief with your line manager or security representative](#) for when you return. Travel approval might be conditional on having a debrief after the trip. If your trip involved visiting a 'special attention' country listed in [Part One](#), a debrief when you return is mandatory.
 7. Check if you need to do anything to prepare for [International Roaming](#). Refer to the [International Roaming](#) section.
 8. **Take a copy of this guidance**; it includes useful contact details that help in the event of a problem while travelling.

On your return

When you return from your trip, you might need to attend a debrief with your line manager or security representative. The purpose of the meeting is to review events and identify anything that needs further attention or action from a security perspective.

In addition to confirming the dates and countries visited, the debrief asks questions such as:

- Did you have any problems arriving at or departing from each country visited?
- Did you have any unusual experiences while travelling, for example actual or suspected surveillance, customs inspections, or removal or disturbance of property?
- Did you have to make any changes to your planned travel arrangements?
- Were you asked unusual or detailed questions about your role, your work, or the MoJ?
- Were there any attempts to bribe, influence, or in some way compromise you, your family, or your colleagues?
- Were you invited to make or maintain on-going contact with a foreign national?
- Were you the victim of any criminal act, or detained or arrested?
- Did you lose or misplace any official material or personal items?
- Did you require medical treatment or legal assistance during your travel?
- Were there any technical difficulties during your travel?

Remain vigilant. In particular, [report](#) any approaches or foreign contacts if they occur in the future.

International Roaming

While travelling, you might incur roaming charges when using your MoJ equipment for calls or accessing services. These charges must be paid by your Business Unit. This is another reason for having a good business need to take MoJ equipment overseas.

By default, MoJ equipment is not enabled for use overseas. Before travelling, request the ServiceNow Catalogue item for International Roaming, and the remote wipe function. This helps protect the MoJ equipment in case of loss or theft.

Note: International Roaming can be found on [Service Now](#) using: **Home > Order IT > Telephony > Mobile Devices > Request for International Roaming**.

If you have any problem when using MoJ equipment overseas

Contact the [IT Service Desk](#) immediately. Tell them if the MoJ equipment is lost, stolen, or was potentially compromised. This includes any time the equipment is deliberately removed out of your sight, such as by a customs official.

If any security-related incident occurs overseas, regardless of whether it involves MoJ equipment, you should contact security@justice.gov.uk as soon as possible. Refer to the following [Contacts](#) section, and the guidance on [Reporting](#)

a [Security Incident](#) on the MoJ Intranet. This includes information on reporting an incident outside of UK working hours. For convenience, the out-of-hours telephone number for reporting incidents is repeated [in this guidance](#).

If there is a problem with your MoJ equipment, it might be necessary to disable your ability to connect to the MoJ network or services from your device. The IT Service Desk will do this if required. MoJ-issued phones might still have some functionality, to let you make phone calls, but the device should be treated as compromised and not used any more for any MoJ business.

Note: Do not be tempted to use non-MoJ equipment for MoJ business purposes. If you are having problems with MoJ equipment, you might wonder about using non-MoJ devices to carry out a particularly important task, or to respond to an urgent email. This is not [acceptable](#).

Related pages

- [General advice on taking equipment overseas](#)
- [Overseas travel](#)
- [Staff security and responsibilities during employment](#)

External websites

- [Foreign and Commonwealth Office: travel and living abroad](#)

Contacts

Security Team

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

IT Service Desk

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

- Tel: 0800 917 5148
- [MoJ Service Portal](#)

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.

Information Incident Reporting Line

- Tel: +44 (0)20 3334 0324 for HMPPS staff at any time.
- Tel: +44 (0)20 3334 0324 for MoJ staff **outside UK working hours**.

During UK working hours, MoJ (but not HMPPS) staff should follow the process on the [Reporting a Security Incident](#) page on the MoJ Intranet.

MoJ Security

- Email: security@justice.gov.uk

General advice on taking equipment overseas

As a government official travelling overseas, you should consider that you are highly likely to be of interest to a range of hostile parties, regardless of your role or seniority. Laptops, tablets and phones are very desirable pieces of equipment to steal and travelling overseas with it puts you at a greater security risk of being a victim of theft.

You should never put yourself in any danger to protect the security of an IT device, as the level of impact to the Ministry of Justice (MoJ) of a compromise does not warrant the risk of injury or loss of liberty. By following your department policies and the advice issued, you can help reduce the risk to yourself and your colleagues.

General guidance

Remove unnecessary files from your device when travelling overseas so that the risk of data exposure is reduced in case of loss or theft.

Keeping safe whilst conducting sensitive work overseas

Be aware that voice calls and SMS messages are not secure and voice calls can be intercepted whilst overseas. Keeping your phone with you at all times helps in having a high level of physical control over the equipment:

- Keep any password/PIN separate from the device.
- Be careful when using your device in situations where it may be lost or stolen, such as busy public places and while transiting customs or security at airports.
- Think about where you are working to ensure that you are not being observed (for instance, somebody looking over your shoulder in a crowded place).
- Never leave the device unattended - not even for a moment.
- If it is not practical to keep the device with you securely at all times (for instance, you are at the swimming pool or gym), consider storing the device in the hotel safe.

Note: Standard hotel safes are not entirely secure and it is normally possible for hotel staff to override controls to gain access. In addition therefore you should also store your device in a tamper proof envelope. You should ensure you have a sufficient number to last the duration of your period of travel. If the tamper evident seals show signs of disturbance or the device exhibits strange behaviour, it should be considered compromised. In either case, you must discontinue use of the device and contact your IT Service Desk immediately and report the device as potentially compromised.

Guidance on using mobile phones

As a government official you may be of interest to a range of hostile parties and therefore:

- If it is not practical to keep the device with you securely at all times (for instance, you are at the swimming pool or gym), consider storing the device in the hotel safe.
- Avoid conducting work related sensitive phone conversations as they can be intercepted and if you do, ensure you can't be overheard. Examples of sensitive information might include prisoner/offence details, court cases of foreign nationals, terror attacks and extremists.
- Do not use public charging stations or connect the phone to a vehicle by USB or Bluetooth as information can be downloaded from your phone.
- Be aware that hotel and public wifi spots are not secure, as they can easily be monitored.
- Make sure you use the phone's password or PIN.
- If the phone is taken from you or you believe it may have been compromised in any way, report it to the [Departmental Security Officer](#).

What to do if you are asked to unlock the device by officials

The extent to which an individual wishes to prevent the customs or security staff from accessing the data will directly relate to its sensitivity. Do not risk your own safety. If the device is being carried by hand to an overseas destination, the sensitivity of the data it holds should not justify any risk to personal safety.

- Try to establish your official status and good faith from the outset.
- Remain calm and polite at all times.
- Carry the names and telephone numbers of a relevant departmental contact and invite the official(s) to contact them to confirm that you are who you claim to be.
- If the official continues to insist on the user inputting his/her password, repeat the previous steps.
- State that you are carrying official UK government property that is sensitive and that you cannot allow access.
- Ask for a discussion with a senior officer or supervisor. You may want to take the names and/or contact details of any officials involved in the event that you wish to pursue a complaint, or an investigation is required, even at a later date.

If you are on official business:

- State that you are a UK civil servant etc. travelling on HMG official business.
- Where appropriate, produce an official document (e.g. on headed notepaper or with a departmental stamp) or identity card that clearly gives your name, photograph and affiliation.
- Produce a letter of introduction from the overseas organisation or individual you are visiting.
- Carry the names and telephone numbers of the officials to be visited in your destination and invite the official(s) to contact them to confirm that you are who you claim to be.

In the event that a device is removed out of your sight (such as by a customs official) then it should be considered compromised. You must [contact the IT Service Desk immediately](#) and report the device as potentially compromised.

The IT Service Desk will disable your ability to connect to the MoJ network from your device. Be aware that although the device will still work as a mobile phone, it should be treated as compromised and not used for any MoJ business.

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.

If unsure, contact your Line Manager.

General enquiries, including theft and loss

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

- Tel: 0800 917 5148
- [MoJ Service Portal](#)

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](#)

Overseas travel

If you are going on a work trip or holiday overseas and you need to take your Ministry of Justice (MoJ) IT devices, you must remain vigilant especially when visiting high risk countries.

As a government worker with access to sensitive information, you are at risk from espionage, intellectual property theft and a range of other threats from hostile third parties as well as foreign intelligence services. These risks can increase when you are overseas, as detailed in the [MoJ Overseas Travel Guide](#).

Before you travel on business, you must seek approval from your Senior Line Manager. You must also inform the security team fifteen days before either a holiday or business trip if you are travelling to or through high-risk countries.

If you are subject to a STRAP briefing you must notify the security team of your intended travel to or through any country (excluding countries in Western Europe, North America, Australia or New Zealand).

The [MoJ Overseas Travel Guide](#) provides detailed guidance before you travel.

Mobile roaming should be requested via the [Service-Now IT Catalogue](#).

Documents

- [MoJ Overseas Travel Guide](#).
- [Overseas travel form](#)
- [Overseas working decision tree](#) – Step by step guide on how you can request to work remotely overseas during COVID-19.

Related pages

- [Remote working – during COVID-19](#)

External websites

- [Foreign, Commonwealth and Development Office \(FCDO\)](#)

Contacts

- security@justice.gov.uk
- [MoJ Group Security](#)

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 135

Overview

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

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

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

In unusual circumstances, it might not be possible to organise provision of equipment. In such cases, you **CAN** request access to an MoJ [virtual environment](#).

Except when connecting to an MoJ [virtual environment](#), or with documented approval in exceptional circumstances as described [in this guidance](#), you **SHALL NOT** use a personal device for work purposes.

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

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

Personal devices **SHALL NOT** be charged from the USB ports of an MoJ device.

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

Guidance

- If you have an MoJ-issued device or virtual environment, you **SHALL** use that.
- You **SHALL NOT** use a personal device to access Google Workspace tools such as Gmail, Docs, Slides, Sheets, Drive, Meet, or Hangouts for work purposes.
- You **SHALL NOT** use a personal device to access Office 365 tools such as Outlook email or calendar, Word, Excel, or PowerPoint for work purposes.

- Wherever possible, an MoJ work device **SHOULD** be used to join business Teams calls, either via video or dial in.
- In cases where staff have not been provided with a work phone or laptop or any other work device which allows them to join or dial into Teams, staff **MAY** join from their personal devices as a Guest. The chair of the meeting **SHALL** confirm the identity of each and every person joining their call as a Guest.
- This guidance applies to all tools accessed through a web browser or installed client applications.
- You **SHALL NOT** send MoJ information to your personal email account.
- You **SHALL NOT** use personal accounts for work purposes.
- You **SHALL NOT** store work files or information on a personal device such as a desktop, laptop, tablet or phone.
- You **SHALL NOT** store work files or information on a personal storage device or memory stick, such as an external drive, thumb drive, or USB stick.
- Some teams within the MoJ **MIGHT** have permission to use personal devices for some tasks. This permission continues, but is being reviewed on an on-going basis. Ensure that you have documented approval recording your permission. Ensure that the permission is no more than 12 months old. To request or refresh permission, ask your Line Manager to seek approval by checking with the [Security team](#).

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

Virtual environment

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

Request a virtual environment through the [Creation of WVD instances](#) product offering within the Service Catalogue in MoJ Service Now.

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

Connected vehicles

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

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

Additionally, although such platforms usually offer an option to delete paired profiles, there is currently no confirmation that the data is actually erased to a satisfactory level. The usual claim is only that the transferred data is deemed inaccessible to the platform menu.

For these reasons, MoJ devices **SHALL NOT** be paired with Bluetooth-enabled vehicles.

Contact details

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

Human resource security

Prior to employment

Minimum User Clearance Requirements Guide

This Minimum User Clearance Requirements Guide outlines the level of security clearance required for staff in order to access specific account types.

Security clearance levels

The Ministry of Justice (MoJ) uses the [national security vetting clearance levels](#):

- Baseline Personnel Security Standard (BPSS)
- Counter Terrorist Check (CTC)
- Security Check (SC)
- Developed Vetting (DV)

Where appropriate, Enhanced checks apply, for example Enhanced Security Check (eSC).

Minimum user clearance requirements

Most of the MoJ IT systems are able to process OFFICIAL information. Therefore all roles in the MoJ require staff to attain BPSS clearance as a minimum to be granted access rights to view OFFICIAL information. Some roles require staff to have higher clearance.

For an individual to perform any of the following tasks, clearance higher than BPSS is required:

- Has long term, regular, unsupervised access to data centres or communications rooms.
- Has regular privileged unsupervised and unconstrained access to systems which contain data for multiple MoJ systems, for example backups, or console access to multiple cloud services.
- Has cryptography responsibilities and handling, under advice from the Crypto Custodian.
- Has access to multiple system security testing outcomes which reveal vulnerabilities in live services.
- Has a role such as system support or IT investigation role, such that without further authority or authorisation, an individual might:
 - Act as another user.
 - Obtain credentials for another user.
 - Directly access other users' data.

If an individual does not need to perform any of the previous tasks, then BPSS, DBS or Enhanced Check is sufficient.

The MoJ HQ and Executive Agencies might have additional, specific requirements for DV/DV STRAP clearance for individual systems. These requirements should be followed where applicable.

Please contact the Cyber Assistance Team and refer to the [Vetting Policy](#) for further information.

Contact details

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

National Security Vetting for External Candidates FAQ

This document provides recruiting managers with answers to frequently-asked questions regarding National Security Vetting for external candidates.

The processes described in this document are under continual review as part of the Ministry of Justice (MoJ) "simpler processes" activities. These FAQs will be updated as required.

Section 1: Directly employed staff

Q1. How does the vacancy manager know what level of clearance a role requires?

Vacancy managers **SHALL** always advertise their roles with the correct level of clearance required. Levels of clearance are defined by the requirements of the role being filled, not by the level of clearance the candidate already possesses. Your National Security Vetting Contact (NSVC) can confirm whether your role requires national security vetting in addition to pre-employment checks. Wrongly classifying roles at advert stage leads to delays in on-boarding.

If you don't know who your NSVC is, refer to the download [here](#).

Q2. What is the pre-employment check process?

This depends on how the candidate is being recruited and their level in the organisation.

Bands A-F (non-SCS) recruited through fair and open recruitment

- All candidates **SHALL** undergo pre-employment checks relevant to the role.
- SSCL will inform applicants to bring their Right To Work (RTW), ID and address documentation to interview.
- Line managers **SHALL** check these documents, make a note of the document reference numbers and input these into Oleo at the Interview Scores Entered stage.
- If the applicant is successful at interview, SSCL will make a provisional offer and ask the candidate to upload copies of the same RTW, ID and address documents into Oleo.
- If NSV is required for the role (as indicated by the vacancy manager in the advert), SSCL will also send a link to the candidate so they can complete an on-line security questionnaire on the NSVS portal.

SCS Grades

- The MoJ SCSBP team work closely with the Government Recruitment Service (GRS), who manage the SCS recruitment campaigns through open and fair competition.
- GRS notify the MoJ SCSBP Team of the successful candidate at interview stage.
- The MoJ SCSBP team contact the candidate to initiate the on-boarding process and send the candidate forms to complete so that SSCL can prepare and issue their contract.
- SCSBP team also arrange a date to meet the candidate and verify their identity documents. These details are used to complete the Clearance Request Form (CRF) and send this to SSCL through the NSVC in the business area.
- Once SSCL process the CRF, a link is sent to the candidate in an email to complete the required security checks on the NSVS portal.

Non-directly employed staff

Refer to [Section 2](#).

Q3. How long do the pre-employment and vetting checks take?

Clearances can involve multiple teams depending on the level of check.

If all information and the correct documents have been provided, the timescales are:

- Baseline Personnel Security Standard (BPSS): average six days.
- Disclosure Barring Service (DBS) standard checks: New checks: average five days.
- Disclosure Barring Service (DBS) enhanced checks: New checks: average six days.
- Counter terrorist check (CTC): new checks: minimum six weeks.
- Security clearance (SC): new checks: minimum six weeks.
- Developed vetting (DV): new checks: minimum 18 weeks.

Although the majority of DBS enhanced checks are completed in six working days, in some parts of the country police authorities quote an estimated response time of six to seven weeks.

Section 2: Staff recruited from external sources (non-directly employed)

As well as any clearance, all staff joining the MoJ from external sources (non-directly employed) are required to complete a BPSS check.

Non-directly employed workers include the following:

- Consultants.
- Contractors.
- Agency staff.
- Fee-Paid workers.

Managers **SHALL** ensure that these applicants undergo the mandatory BPSS checks covering: identity, nationality, immigration, Right To Work (RTW), employment history, and criminal records checks. SSCL will not conduct these checks.

For posts that require NSV:

- The vacancy manager **SHALL** discuss this with their NSVC and obtain a code which needs to be entered on the CRF submitted to SSCL.
- If you don't know who your NSVC is, refer to the download [here](#).
- SSCL only accepts requests with a valid vetting reference code provided on the CRF.
- SSCL sends a link to the candidate so they can complete their on-line security questionnaire on the NSVS portal.

To progress NSV applications, SSCL requires evidence of completion of BPSS checks from the contractor or agency before NSV can be initiated. If you need more information, contact SSCL on 0845 241 5359 (option 1).

Section 3: National security vetting

Q1. What is National Security Vetting (NSV)?

There are three levels of national security clearance:

- Counter terrorist check (CTC).
- Security clearance (SC).
- Developed vetting (DV).

These are mandatory for certain job roles and locations throughout the MoJ.

You need the appropriate level of national security clearance if:

- You have a proximity to public figures who have been assessed to be at risk from terrorist attack.
- You work in a role which has the potential to cause significant damage to MoJ or its assets.

Q2. How long does national security vetting take?

Refer to [Q3, Section 1](#).

Q3. National Security Vetting takes too long, can the candidate start at BPSS and apply for NSV once they are in post?

If NSV is required for a position, candidates **SHOULD NOT** start until their NSV is confirmed.

In exceptional circumstances, a policy dispensation request can be made to mojgroupsecurity@justice.gov.uk, who will give a recommendation on whether to grant or refuse the request. Any risk mitigation measures deemed to be required will also be provided for the Senior Security Advisor and the business unit to sign-up to.

Contractors and Agency staff, who **SHALL** have their NSV in place before they start, should contact their NSVC in the first instance. If you don't know who your NSVC is, refer to the download [here](#).

Section 4: National Security Vetting Applications

Q1. I submitted an NSV request several weeks ago, how do I find out its status?

If you require confirmation of the security clearance level, ask your NSVC who will make enquiries for you. If you don't know who your NSVC is, refer to the download [here](#).

Q2. SSCL have told me that they have completed sponsors' actions, what does that mean?

It means that your security questionnaire has been forwarded to United Kingdom Security Vetting (UKSV), and the vetting process has started. All actions are complete at the MoJ, and there are no further actions until UKSV return the file with a decision.

Q3. Why is the candidate required to fill in forms on the NSVS portal, and provide information that may already be held elsewhere in the recruitment process?

NSV is a separate process and is not HR-related. For legal reasons, we often ask questions to confirm facts. Even if we have that information elsewhere, we still require confirmation. It is usually easier to gather everything we need in one process; the alternative would be to repeatedly ask for further information. Experience has shown that this causes significant delay. We don't ask for information that we do not need.

Q4. What if the candidate doesn't complete specific dates and details for the Security Questionnaire?

All information declared on the Security Questionnaire **SHALL** be completed in full and to the best of the candidate's knowledge. If certain dates or information are not known, they should include an explanation in the information box provided. Missing or incorrect data delays the application, as the file is referred to a vetting officer who needs to investigate and find the missing data.

Q5. What happens if the candidate misses information out?

We cannot give too much detail about the vetting process for security reasons. However, we can confirm that your information is checked in a variety of systems and databases. If information is mismatched, it forces the file to be referred to a vetting officer. This intervention causes significant delay. Thirteen percent of all NSV cases are rejected because the subject doesn't provide their official middle name(s). It is also not unusual for people to put the wrong date of birth.

It is crucial that accurate information is provided. It really helps vet people more quickly.

Q6. My candidate applied for national security vetting some time ago and hasn't heard anything, who can I check this with?

SC/CTC each take a minimum of six weeks, with an average of nine weeks. DV takes at least 18 weeks. If this time frame has passed, contact the NSVC who requested the clearance. They can contact SSCL for an update.

If you don't know who your NSVC is, refer to the download [here](#).

Q7. Why can't candidates use Apple products to submit the security questionnaire?

NSVS is run by UKSV. There are very strict controls in place to make certain that the information you provide is secure. Apple products work in a different way. UKSV can't be assured, by Apple, that their platform is secure.

We do not expect that this will change in the foreseeable future.

Section 5: Changes to roles or personal circumstances

This section contains information for managers and staff who are already in the MoJ, and have changes to their roles or personal circumstances:

Q1. I am a manager and I think a member of my team needs a national security vetting clearance to do a new piece of work. What should I do?

Talk to your National Security Vetting Contact (NSVC). All business areas that have at least one member of staff who holds Security Clearance should have one. If you don't know who your NSVC is, refer to the download [here](#).

Q2. My national security vetting clearance is going to expire soon, what should I do?

Speak to your national security vetting contact (NSVC), they will decide if it needs to be renewed and help you start the process off. If you don't know who your NSVC is, refer to the download [here](#).

Q3. My personal circumstances have changed, who should I advise?

For all changes in personal circumstances, please contact Cluster 2 Personnel Risk Management by emailing: VettingAftercare@cluster2security.gov.uk. Failure to report relevant changes could result in withdrawal of clearance.

Contact details

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

National Security Vetting contact

All business areas in the Ministry of Justice (MoJ) **SHALL** enrol or appoint a National Security Vetting Contact (NSVC) to help business areas progress and monitor applications for security clearance.

Most applications for National Security Vetting (NSV) clearance including Counter Terrorist Clearance (CTC), Security Check (SC), and Developed Vetting (DV) come through recruitment campaigns or are agency staff or contractors.

Some business areas employ large number of NSV-cleared people and those clearances need to be managed and monitored. The MoJ recognises that many personnel are contractors and agency staff, often with clearances held elsewhere. The NSVC **SHALL** facilitate the process and provide the business with a single point of contact and liaison with the National Security Vetting Team and Shared Services Connected Limited (SSCL).

Roles and responsibilities

- NSVCs are a mandatory role and one **SHALL** be appointed if there are National Security Vetted staff in any business area.
- NSVCs **SHALL** undergo the Baseline Personnel Security Standard (BPSS) check as a minimum, and be registered with [MoJ Group Security](#). How many NSVCs a business area needs is for Senior Managers to determine, based on how they are organised. For example, how many NSV clearances need processing and maintenance.
- NSVCs monitor the progress of all applications for an NSV clearance and **SHALL** maintain a register of all active NSV personnel within their business area.
- NSVCs **SHALL** provide the authorisation and complete the SSCL [Clearance Request Form](#) that confirms the level of clearance required for that person. SSCL will not process an application if an NSV matrix code is not supplied by the NSVC.
- NSVCs act as a single point of contact for their business area for SSCL and MoJ security to speed up the NSV process.

For further information regarding roles, responsibilities and necessary security clearances, contact mojgroupsecurity@justice.gov.uk.

Registration

- To register with [MoJ Group Security](#), complete the [Registration Form in the Downloads section](#) at the bottom of this page, and return it to the email address provided in the form.
- On registration, [MoJ Group Security](#) provides the NSVC with the documents they need to manage the process and confirm registration with SSCL.

Downloads

The following downloads are available from the MoJ Intranet.

- [National Security Vetting contact guide](#).
- [National Security Vetting contact registration form](#)
- [National Security Vetting contacts register](#).

National Security Vetting questions

The processes described in this document are under review as part of Ministry of Justice (MoJ) "simpler processes" activities and these FAQs will be updated as required.

A downloadable version of this document is available [here](#).

National Security Vetting

What is National Security Vetting?

There are three levels of National Security Vetting (NSV) or clearance:

- Counter Terrorist Check (CTC).
- Security Check (SC)
- Developed Vetting (DV)

These are mandatory for certain job roles and locations throughout the MoJ.

You need the appropriate level of national security clearance if:

- You have a proximity to public figures who have been assessed to be at risk from terrorist attack.
- You work in a role which has the potential to cause significant damage to the MoJ or its assets.

Can NSV clearance be transferred from another government department?

Candidates cannot choose to transfer their NSV clearance, which lapses on their last day of employment. The MoJ determines what NSV is required for **the new role** and, if necessary, requests that a candidate's NSV clearance is transferred over before starting a new application for NSV. Not all other government department (OGDs) agree to transfer or share; it is their choice and there are various reasons for transferring or not transferring.

Three scenarios are given here:

Scenario 1: The level of clearance required for the new role is the same level the exporting department held for the individual.

For example, the new role requires SC clearance, and the candidate's exporting department held valid SC clearance for them.

Answer: Transfer can take place provided the exporting department confirms a valid NSV clearance **and** agrees to transfer it to the MoJ. In most cases these transfers can take place. In some exceptional circumstances, departments may refuse to transfer clearance to the MoJ. Where this happens, the candidate is required to complete NSV again.

Scenario 2: The level of clearance required for the new role is higher than the level the individual possesses in their current department.

For example, the role requires SC clearance and the current department holds CTC.

Answer: As the level of clearance is higher, the employee is required to complete an application for the new level on the NSV portal. A link is sent to them by SSCL once they have accepted a provisional offer.

Scenario 3: The level of clearance required for the role is lower than the current department holds.

For example, the employee currently possesses DV clearance with their present department but their new post in MoJ requires SC.

Answer: For security reasons, the MoJ **CAN NOT** transfer the higher level of clearance as the **role** does not require it. However, information is extracted to ensure that the candidate is not required to re-apply for a lower level of transfer. This is subject to the current department agreeing to transfer.

Can a candidate start work before applying for NSV?

If NSV is required for a position, candidates **SHOULD NOT** start until their NSV is confirmed.

In exceptional circumstances, a policy dispensation request can be made to [MoJ Group Security](#), who will provide a request form and then give a recommendation on whether to grant or refuse the request. Any risk mitigation measures deemed to be required (such as plans to segregate the candidate from data that they don't have clearance to see) will also be provided for the Senior Security Advisor and the business unit to sign-up to.

As a minimum requirement, a candidate **SHALL** have submitted their Security Questionnaire on the NSVS portal. This does not extend to Contractors and Agency staff, who **SHALL** have their NSV in place before they start. If you don't know who your NSVC is, refer to the download [here](#).

Directly employed staff

How does the vacancy manager know what level of clearance a role requires?

Vacancy managers must always advertise their roles with the correct level of clearance required. Levels of clearance are defined by the requirements of the role being filled, and not by the level of clearance the candidate already possesses. Your NSVC can confirm whether your role requires national security vetting in addition to the usual pre-employment checks. Wrongly classifying roles at advert stage will lead to delays in on-boarding.

If you don't know who your NSVC is, refer to the download [here](#).

What is the pre-employment check process?

The checks required depend on how the candidate is being recruited and their level in the organisation.

Bands A-F (non-SCS) recruited through fair and open recruitment

- All candidates must undergo pre-employment checks relevant to the role, although staff transferring from OGDs have simplified checks.
- SSCL will ask applicants to bring their Right to Work, ID and address documentation to interview.
- Line managers must check these documents, make a note of the document reference numbers and input these into Oleo at the Interview Scores Entered stage.
- If the applicant is successful at interview, SSCL will make a provisional offer and ask the candidate to upload copies of the same RTW, ID and address documents into Oleo.
- If National Security Vetting (NSV) is required for the role (as indicated by the vacancy manager in the advert), SSCL will also send a link to the candidate so they can complete an on-line security questionnaire on the National Security Vetting Service (NSVS) portal.
- If the candidate already has any NSV clearances (and has noted this in their pre-appointment form), it may be possible to transfer these to the new role.

Bands A-F (non-SCS) recruited as exception to fair and open recruitment

- These include managed moves and loans and are not advertised in Oleo.
- The vacancy manager should arrange for the individual to bring their original Right to Work, ID and address documentation to be checked.
- The vacancy manager should then submit a Clearance Request Form (CRF) to SSCL recording the details of these documents.
- SSCL send the successful candidate a provisional offer with links to the "Lumesse" system where they must upload the same documents.
- If NSV is required for the role, the vacancy manager must discuss this with their NSVC and obtain a code which needs to be entered on the CRF. SSCL will only accept requests with a valid vetting reference code provided on the Clearance Request Form.
- SSCL will send a link to the candidate so they can complete their on-line security questionnaire on the NSVS portal.
- If the candidate already has any NSV clearances, it may be possible to transfer these to the new role.

SCS Grades

- The MoJ Senior Civil Service Business Partners (SCSBP) team work closely with the Government Recruitment Service (GSR), who manage the SCS recruitment campaigns through open and fair competition.
- GSR notify the MoJ Senior Civil Service Business Partners (SCSBP) Team of the successful candidate.
- The MoJ SCSBP team contact the candidate to initiate the on-boarding process and send the candidate forms to complete so that SSCL can prepare and issue a contract.
- SCSBP team also arrange a date to meet the candidate and verify their identity documents. These details are used to complete the CRF and send this to SSCL via the NSVC in the business area.
- Once SSCL process the CRF, a link is sent to the candidate via an email to complete the required security checks on the NSVS portal. This process is also used to transfer existing clearances for OGD candidates.

How long do the pre-employment and vetting checks take?

Clearances can involve multiple teams depending on the level of check.

If all information and the correct documents have been provided, the timescales are:

- Baseline Personal Security Standard (BPSS): average six days.
- Disclosure Barring Service (DBS) standard checks: New checks: average five days.
- Disclosure Barring Service (DBS) enhanced checks: New checks: average six days.
- Counter terrorist check (CTC): new checks: minimum six weeks.
- Security check (SC): new checks: minimum six weeks.
- Developed vetting (DV): new checks: minimum 18 weeks.

Although the majority of DBS enhanced checks are completed in six working days, in some parts of the country authorities estimate a response time of six to seven weeks.

Non-directly employed

As well as any clearance, all staff joining the MoJ from external sources (non-directly employed) are required to complete a BPSS check. SSCL will not conduct these checks and it is the recruiting manager's responsibility to ensure that they are done.

Further guidance, and a link to the BPSS Verification Form, can be found on the MoJ Intranet [here](#).

Non-directly employed workers include the following:

- Consultants.
- Contractors.
- Agency staff.
- Fee-Paid workers.

For posts that require NSV:

- The vacancy manager must discuss this with their NSVC and obtain a code which needs to be entered on the CRF submitted to SSCL.
- If you don't know who your NSVC is, refer to the download [here](#).
- SSCL will only accept requests with a valid vetting reference code provided on the CRF.
- SSCL will send a link to the candidate so they can complete their on-line security questionnaire on the NSVS portal.

To progress NSV applications, SSCL require evidence that BPSS checks have been completed from the contractor/agency before NSV can be initiated. If you need more information contact SSCL on 0845 241 5359 (option 1).

National Security Vetting Applications

Why are candidates asked to repeat information supplied elsewhere in the recruitment process?

NSV is a separate process and is not HR-related. For legal reasons, we often ask questions to confirm facts. Even if we have that information elsewhere, we still require confirmation. It is usually easier to gather everything we need in one process; the alternative would be to repeatedly ask for further information. Experience has shown that this causes significant delay, and we don't ask for information that we do not need.

What happens if the candidate misses information out?

All information declared on the Security Questionnaire must be completed in full and to the best of the candidate's knowledge. If certain dates or information are not known, they should include an explanation in the information box provided. Missing or incorrect data delays the application as the file is referred to a vetting officer who must investigate and find the missing data.

We cannot give too much detail about the vetting process for security reasons; however, we can confirm that your information is checked in a variety of systems and databases. If information is mismatched, it forces the file to be referred to a vetting officer, this intervention causes significant delay. Thirteen percent of all NSV cases are rejected because the subject doesn't provide their official middle name(s). It is also not unusual for people to put the wrong date of birth. It is crucial that accurate information is provided, it really helps vet people more quickly.

How do I check the progress of an application?

SC/CTC takes a minimum of six weeks, and DV takes at least 18 weeks. If this time frame has passed, contact the NSVC who requested the clearance, they will contact SSCL for an update.

Why can't Apple products be used to submit the security questionnaire?

NSVS is run by UKSV and there are very strict controls in place to make certain that the information you provide is secure. Apple products work in a different way and UKSV can't be assured, by Apple, that their platform is secure.

We do not expect that this will change in the foreseeable future.

Changes to roles or personal circumstances

This section contains information for managers and staff who are already in the MoJ and have changes to their roles or personal circumstances.

How do I decide if a new piece of work requires staff to have NSV?

If you need to decide if a new piece of work requires clearance, talk to your NSVC. All business areas that have at least one member of staff who holds Security Clearance should have one. If you don't know who your NSVC is, refer to the download [here](#).

How do I renew NSC?

If your, or one of your staff's, NSC is due to expire soon, speak to your NSVC, they will decide if it needs to be renewed and help you start the process off. If you don't know who your NSVC is, refer to the download [here](#).

If my personal circumstances change, who do I tell?

For all changes in personal circumstances please contact Cluster 2 Personnel Risk Management by emailing: VettingAftercare@cluster2security.gov.uk. Failure to report relevant changes could result in withdrawal of clearance.

You can find more information [here](#).

Contact details

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

Pre-employment screening

Pre-employment screening involves a series of checks to help us make informed decisions about the suitability of individuals to work for the Ministry of Justice (MoJ) and its agencies. These checks ensure the following:

- Compliance with current legislation, for example evidence of Right to Work in the UK
- That applicants are who they say they are.
- The integrity of the applicant, our organisation, and the safety of staff and individuals in our care.

Pre-employment screening procedures are required for all people applying for posts or working within the MoJ, including:

- [Directly employed staff](#).
- [Staff transferring from Other Government Departments \(OGD Transfers\)](#).

FAQs

- [Pre-employment screening and Vetting FAQs](#)

Downloads

- [Applying criminal records checks](#)

Contact details

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

Pre-Employment Screening and Vetting of External Candidates - FAQs

This document describes pre-employment screening and National Security Vetting when recruiting External Candidates.

It answers Frequently Asked Questions (FAQs) for recruiting managers.

A downloadable version of this information is available [here](#).

Section 1: Pre-employment screening for directly employed staff

Q1. What is pre-employment screening?

Pre-employment screening involves a series of checks to help us make informed decisions about the suitability of people to work for the Ministry of Justice (MoJ) and its agencies. These checks ensure:

- Compliance with current legislation, for example evidence of right to work in the UK.
- That applicants are who they say they are.
- The integrity of the applicant, the organisation, and the safety of staff and others in our care.

All individuals working with the MoJ **SHALL** be required to complete a Baseline Personnel Security Standard (BPSS) check prior to taking up their role.

In addition, Disclosure and Barring Service (DBS) clearances might be required but only where the role involves interaction with children or vulnerable adults. These clearances are carried out through either a Standard or an Enhanced check.

National Security Vetting (NSV) might be required but only where the role requires Counter Terrorist Check (CTC), Security Clearance (SC) or Developed Vetting (DV) clearance. Refer to [Section 2](#) for more information. **NSV** is separate and additional to pre-employment screening checks.

Q2. What is BPSS?

Baseline Personnel Security Standard (BPSS) is the minimum level of clearance for all people working across the Civil Service. A BPSS check comprises of the following components or checks:

- Confirmation of right to work in the UK.
- Confirmation of ID and address.
- Eligibility.
- Criminal convictions.
- Employment history.
- Counter-signatory reference (where relevant).
- Health check (where relevant).

Q3. How does the vacancy manager know what level of clearance a role requires?

Vacancy managers **SHALL** always advertise their roles at the correct level of clearance required. Levels of clearance are defined by the requirements of the role being filled, not by the level of clearance the candidate already possesses. Your National Security Vetting Contact (NSVC) can confirm whether the role requires national security vetting in addition to pre-employment checks. Wrongly classifying roles at advert stage leads to delays in on-boarding.

If you don't know who your NSVC is, refer to the download [here](#).

Q4. What is the process for completing pre-employment checks?

This depends on how the candidate is being recruited, and their level in the organisation.

Bands A-F (non-SCS) recruited through fair and open recruitment

- All candidates **SHALL** undergo pre-employment checks relevant to the role.
- SSCL ask applicants to bring their Right to Work (RTW), ID, and address documentation to interview.
- Line managers **SHALL** check these documents, make a note of the document reference numbers, and input these into Oleo (the recruitment website), at the Interview Scores Entered stage.
- If the applicant is successful at interview, SSCL makes a provisional offer, and asks the candidate to upload copies of the same RTW, ID, and address documents into Oleo.
- If NSV is required for the role (as indicated by the vacancy manager in the advert), SSCL also sends a link to the candidate so they can complete an on-line security questionnaire on the NSVS portal.

SCS Grades

- The MoJ SCSBP team work closely with Civil Service Resourcing (CSR), now called Government Recruitment Service (GRS), who manage the SCS recruitment campaigns through open and fair competition.
- GSR notify the MoJ SCSBP Team of the successful candidate at interview stage.

- The MoJ SCSBP team contacts the candidate to initiate the on-boarding process, and sends the candidate forms to complete so that SSCL can prepare and issue their contract.
- SCSBP team also arrange a date to meet the candidate and verify their identity documents. These details are used to complete the Clearance Request Form (CRF) and send this to SSCL via the National Security Vetting Contact (NSVC) in the business area.
- Once SSCL processes the CRF Form, a link is sent to the candidate by email to complete the required security checks on the NSVS portal.

Non-directly employed staff

Refer to [Section 2](#).

Q5. How long do the pre-employment and vetting checks take?

Any clearances can involve multiple teams and depend on the level of check.

If all information and the correct documents have been provided, the average time for the checks to be completed is:

- Baseline Personnel Security Standard (BPSS): average 6 days
- Disclosure Barring Service (DBS) standard checks: New checks average 5 days
- Disclosure Barring Service (DBS) enhanced checks: New checks average 6 days
- Counter terrorist check (CTC): New checks minimum six weeks, averaging six weeks
- Security clearance (SC): New checks minimum six weeks, averaging six weeks
- Developed vetting (DV): New checks minimum 18 weeks.

Although the majority of DBS enhanced checks are completed in six working days, in some parts of the country police authorities quote a six to seven week response time.

Section 2: Staff recruited from external sources (non-directly employed)

All staff joining the MoJ from external sources (non-directly employed) are required to complete a BPSS check.

Non-directly employed workers include the following:

- Consultants.
- Contractors.
- Agency staff.
- Fee-Paid workers.

Managers **SHALL** ensure that these applicants undergo the mandatory BPSS checks covering identity, nationality, immigration, right to work, employment history, and criminal records checks. They can check the results on the BPSS Verification Record form, which employers **SHALL** complete to verify that the checks have been made.

Note: SSCL do not conduct these checks.

Further guidance, and a link to the BPSS Verification Form, can be found on the MoJ [Intranet](#).

If you have posts that require NSV

If NSV is required for the role, the vacancy manager **SHALL** discuss this with their National Security Vetting Contact (NSVC), and obtain a code that is entered on the Clearance Request Form (CRF) prior to submission to SSCL.

If you don't know who your NSVC is, refer to the download [here](#).

- SSCL only accepts requests with a valid vetting reference code provided on the CRF.
- SSCL sends a link to the candidate so they can complete their on-line security questionnaire on the NSVS portal.

To progress NSV applications, SSCL requires evidence of completion of BPSS checks from the contractor or agency before NSV can be started. If you need more information, contact SSCL on 0845 241 5359 (option 1).

Section 3: National Security Vetting

Q1. What is National Security Vetting (NSV)?

There are 3 levels of national security clearance:

- Counter Terrorist Check (CTC).
- Security Clearance (SC).
- Developed Vetting (DV).

These are mandatory for certain job roles and locations throughout the MoJ.

You need the appropriate level of national security clearance if:

- You have a proximity to public figures who have been assessed to be at risk from terrorist attack.
- You work in a role which has the potential to cause significant damage to the MoJ or its assets.

Q2. How long does national security vetting take?

Typical timings from completion of application are

- Counter Terrorist Check (CTC): New checks minimum six weeks, averaging six weeks.
- Security Clearance (SC): New checks minimum six weeks, averaging six weeks.
- Developed Vetting (DV): New checks minimum 18 weeks.

Q3. NSV takes too long, can the candidate start at BPSS and apply for NSV once they are in post?

If NSV is required for a position, candidates **SHOULD NOT** start until their NSV is confirmed.

In exceptional circumstances, a policy dispensation request **CAN** be made to the Cluster 2 Security Unit (C2SU). Do this by emailing [MoJ Group Security](#). C2SU recommend whether to grant or refuse the request. Any required risk mitigation measures will be provided by C2SU and **SHALL** require the Senior Security Advisor and the business unit to sign-up to these required measures.

Contractors and Agency staff **SHALL** have their NSV in place before they start. For help, contact your NSVC in the first instance. If you don't know who your NSVC is, refer to the download [here](#).

Section 4: Applying for NSV

Q1. I submitted an NSV request several weeks ago, how do I find out where it is?

Contact the SSCL contact centre on 0845 241 5359 (option 1). SSCL are responsible for the registration and sponsoring of all applications for the NSVS portal.

Q2. SSCL have told me that they have completed sponsors' actions, what does that mean?

It means that your security questionnaire has been forwarded to United Kingdom Security Vetting (UKSV), and the vetting process has started. All actions are complete at the MoJ. There are no further actions until UKSV returns the file with a decision.

Q3. Why is the candidate required to fill in forms on the NSVS portal and provide information that may already be held elsewhere in the recruitment process?

NSV is a separate process to anything HR-related. For legal reasons, we often have to ask applicants questions to confirm facts. Even if we have that information elsewhere, we still require the applicant to confirm it. It is usually easier to gather everything we need in one process; the alternative would be to repeatedly return for further information. Experience has shown that this causes significant delay, and we don't ask for information that we would not need.

Q4. What if the candidate doesn't complete specific dates and details for the Security Questionnaire?

All required information on the Security Questionnaire must be completed in full and to the best of the candidate's knowledge. If certain dates or information are not known, an explanation should be added in the information box. Missing or incorrect data will delay the application because the file will be referred to a vetting officer who will have to investigate and find the missing data.

Q5. What happens if the candidate leaves out information?

For security reasons we cannot give too much detail about the vetting process; however, we can confirm that information is checked in a variety of systems and databases. If information is mis-matched, it forces the file to be referred to a vetting officer and this intervention causes significant delay. Thirteen percent of all NSV cases are

rejected because the subject doesn't provide their middle name(s) and it is not unusual for people to put the wrong date of birth. It is crucial that accurate information is provided; it really helps vet people quickly.

Q6. My candidate completed the national security vetting application some time ago and hasn't heard anything, who can I check this with?

SC/CTC takes a minimum of six weeks and DV takes at least 18 weeks. If this time frame has been passed, contact the National Security Vetting Contact (NSVC) who requested clearance and they can contact SSCL for an update.

If you don't know who your NSVC is, refer to the download [here](#).

Q7. Why can't candidates use an Apple machine or iPad to submit the NSV security questionnaire?

NSVS is run by UKSV. There are very strict controls in place to make certain that the information you provide is secure. Apple products work in a different way and UKSV can't be assured by Apple that their platform is secure. We do not expect that will change in the foreseeable future.

Section 5: Changes to roles or personal circumstances

This section contains information for managers, and for staff who are already in the MoJ, regarding changes to roles or personal circumstances.

Q1. I am a manager and I think a member of my team needs a national security vetting clearance to do a new piece of work. What should I do?

Talk to your NSVC. All business areas that have at least one member of staff who holds Security Clearance should have one. If you don't know who your NSVC is, refer to the download [here](#).

Q2. My national security vetting clearance is going to expire soon, what should I do?

Speak to your NSVC. They decide if it needs to be renewed and help you start the process off. If you don't know who your NSVC is, refer to the download [here](#).

Q3. My personal circumstances have changed, who should I advise?

For all changes in personal circumstances, contact Cluster 2 Personnel Risk Management by emailing VettingAftercare@cluster2security.gov.uk.

You can find more information [here](#).

Contact details

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

Security clearance appeals policy

The Cluster 2 Security Unit (C2SU) forms part of the Transforming Government Security programme, which aims to standardise and strengthen operational security across Government.

The Ministry of Justice (MoJ) is part of Cluster 2, and so must adhere to this policy.

This policy applies to permanent members of staff and contractors' employees employed on the work of the MoJ, and those organisations for which the Cluster 2 Security Unit holds the responsibility for vetting, including non-departmental public bodies (NDPBs).

It also applies to:

- Existing contractors' employees or other non-permanent staff, who are already engaged in the work of the MoJ.
- Existing permanent members of staff of other government departments and organisations who have applied for a security clearance with the MoJ.
- Existing contractors' employees already engaged on government work in other departments and organisations who have applied for a security clearance with the MoJ.

It *does not apply* to individuals on initial recruitment to the Civil Service seeking a first security clearance for permanent employment or contractual work with the MoJ.

It *does* include existing employees of a contractor who are newly deployed to contracted work for the MoJ.

Policy

The MoJ provides a right of internal appeal to the Permanent Secretary where an individual who falls within the scope of this policy has a security clearance refused or withdrawn by the Cluster 2 Security Unit. The appeal **SHOULD** be submitted within 15 working days of notification of the refusal or withdrawal decision.

Where the Permanent Secretary upholds the vetting decision to refuse or withdraw security clearance, there is a further avenue of appeal to the independent Security Vetting Appeals Panel (SVAP). This appeal **SHOULD** be submitted within 28 days of notification that the vetting decision has been upheld.

To achieve this requirement, the Cluster 2 Security Unit must:

- Ensure that the decision to refuse or withdraw national security clearance for an existing permanent or contracted employee (as identified previously) is communicated to the individual promptly and in writing.
- Ensure that the individual is given the full reasons for the decision, and the relevant facts upon which it was based, as far as considerations of security and confidentiality allow.
- Provide the employee with a clear explanation of their right to an internal appeal and the mechanisms by which they can make that appeal, and of their entitlement, should they remain dissatisfied with the outcome, to appeal to the Security Vetting Appeals Panel (SVAP).
- Ensure the appeal process will be carried out independently from the vetting decision makers and anyone involved in the original decision to refuse or withdraw clearance. The process will also - as far as issues of national security and confidentiality allow - be undertaken with transparency, providing a fair opportunity for the appellant to address the reasons for the decision.

Further guidance

Detailed guidance on the processes and timescales for internal and external appeals is given in the Security Clearance Appeals Procedures.

More information about the Security Clearance Appeals Procedures can be obtained from [MoJ Group Security](#).

Contact details

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

Security clearance appeals procedures

These procedures provide an overview of the requirements for appealing a decision by the Cluster 2 Security Unit Head of Personnel Security, or their representatives in the Decision Making or Personnel Risk Management Teams, to refuse or withdraw national security clearance for Civil Service and Government employees and contractors working on Cluster 2 business.

There is an internal appeal to the Ministry of Justice (MoJ) Permanent Secretary, and if the decision to refuse or withdraw clearance is upheld, a subsequent external appeal to the Security Vetting Appeals Panel (SVAP).

More detailed guidance on the processes and timescales for internal and external appeals can be found at [Annex A: Cluster 2 Security Unit Security Clearance Appeals Procedures](#).

In this document the term **SHALL** is used to indicate an absolute requirement.

If you have any queries on the content of this document contact [MoJ Group Security](#).

Scope and aim

These procedures apply to permanent members of staff and contractors' employees employed on the work of MoJ, and those organisations for which the Cluster 2 Security Unit holds the responsibility for vetting, including non-departmental public bodies (NDPBs).

It also applies to:

- Existing contractors' employees or other non-permanent staff, who are already engaged in the work of the MoJ.

- Existing permanent members of staff of other government departments and organisations who have applied for a security clearance with the MoJ.
- Existing contractors' employees already engaged on government work in other departments and organisations who have applied for a security clearance with the MoJ.

It does not apply to individuals on initial recruitment to the Civil Service seeking a first security clearance for permanent employment or contractual work with the MoJ.

These procedures apply to existing employees of a contractor who are newly deployed to contracted work for the MoJ.

The Government functional standard for security

[Government Functional Standard - GovS 007: Security](#) sets the expectations for protecting the government's people, information and assets. In respect of personnel security, it states that government organisations **SHALL** deliver the appropriate combination of recruitment checks, vetting and on-going personnel security aftercare to reduce the risk from insider threat. Furthermore, GovS 007 states that government organisations **SHALL** have:

A process in place which defines the approach to handling the refusal or withdrawal of clearances for both candidates at the recruitment stage and those already in employment.

Data sharing

As part of the processing of the appeal, there may be circumstances which require the Appeal Team to discuss aspects of the case with third parties. The team always balances the need to limit the disclosure of sensitive information with the need to progress the case with individuals or departments that are crucial to obtaining a fair and balanced appeal process.

In doing so the team always seeks consent from the individual to share data, subject to national security considerations.

As an example, the MoJ employs a Senior Security Advisor (SSA) who liaises with the Security Unit on behalf of the Permanent Secretary.

The SSA provides information to the Security Unit concerning the role in the MoJ for which security clearance is being sought, thereby identifying the level of risk inherent in employing an individual to that post. The SSA is therefore involved in the national security vetting process in an advisory capacity and is made aware of concerns raised by the Security Unit in the course of that process which might result in a clearance being refused or withdrawn.

The SSA also acts as liaison between the Appeals Team and the MoJ throughout the appeal process.

Upon completion of this process, the Head of Vetting Appeals provides a full report and recommendation to the Permanent Secretary. The SSA is invited to view this report before submission.

The final decision to uphold the appeal or the decision to refuse or withdraw is made by the Permanent Secretary and communicated direct to the appellant.

Note: The appellant is defined as the individual who has had their security clearance refused or withdrawn, and wishes to appeal this decision.

Where necessary, data **CAN** also be shared with the appellant's line manager, or the originator of material gathered in the course of national security vetting which has a bearing on the decision to refuse or withdraw clearance. In so doing, consent is always sought from the individual to share data, subject to considerations of national security.

Contacts

For general advice or guidance regarding the National Security Vetting process, contact [MoJ Group Security](#).

To declare relevant changes in your personal circumstances, contact the Cluster 2 Personnel Risk Management Team by emailing VettingAftercare@cluster2security.gov.uk.

Annex A: Cluster 2 Security Unit Security Clearance Appeals Procedures

Internal appeals

Enclosed with the vetting decision letter to refuse or withdraw CTC (Counter Terrorist Check), SC (Security Check) or DV (Developed Vetting) security clearance **SHOULD** be the appeal documents comprising:

- An explanation of the internal vetting appeals policy and process and of the entitlement, should that appeal fail, to appeal to the independent Security Vetting Appeals Panel (SVAP).
- An internal appeal form ([Annex B](#)) to be completed by the individual, and guidance as to what is required of the individual when lodging an appeal, for example provision of any additional information, identification of the reason(s) for the appeal as well as any alleged 'inaccuracy' or 'misunderstanding' in the decision letter.

The vetting decision letter **SHOULD** also provide clear details of where the appeal notice **SHOULD** be sent.

Appeals **SHALL** be made by the appellant and sent to the Permanent Secretary using the "Internal appeal form following refusal or withdrawal of security clearance" ([Annex B](#)) within 15 working days of receiving the vetting decision.

In lodging an appeal, the appellant **SHOULD** provide as full a rationale as they able, based on the reasons provided in the decision letter, with supporting facts where applicable and including any further information or documentation that **MIGHT** assist their appeal. An appeal submission **MIGHT** include information that was not previously available when the original clearance decision was made, where this information is materially relevant to the case.

On receipt of an appeal, the Permanent Secretary **CAN** delegate the handling of it to an appeal officer, usually the Head of Vetting Appeals in the Cluster 2 Security Unit. The appeal officer is independent: they **SHALL NOT** have had any prior involvement or interest in the original decision-making process. The Permanent Secretary reserves the right to hear an appeal internally at their home department in any circumstances if they consider it appropriate.

The Senior Security Advisor (SSA) of the MoJ acts as liaison between the Appeals Team and their department throughout the appeal process. The appeal officer conducts the appeal on behalf of the Permanent Secretary and provides a report and recommendation to the Permanent Secretary. In all cases, the Permanent Secretary makes the final decision.

The appeal officer conducts the internal appeal according to the following guidelines:

1. They contact the appellant within 5 working days of being delegated to handle the appeal. The appeal officer introduces themselves and provide contact details for the appellant, along with an explanation of the next steps in the appeal process.
2. The appeal officer provides the vetting decision maker (usually either the Head of Vetting Decisions or the Head of Personnel Risk Management, or their representative) with the appellant's grounds of appeal and invites them to provide a statement of case and response to the appellant's representations. They are also asked to provide all documents relevant to the decision and the processes involved.
3. On receipt of the decision maker's statement of case and supporting documentation, an appeal bundle is prepared and sent to the appellant, who is allowed a minimum 10 working days to prepare their response based on the contents of the bundle and their own representations.
4. The appeal officer usually invites the appellant to present their case in person at an appeal hearing. Where this is agreed, the appellant is expected to make themselves available for the hearing as directed. If the appellant chooses not to attend the hearing in person, the appeal is considered on papers alone. If the appellant fails to agree a date for the hearing within six weeks of receiving their papers, or fails to attend the agreed hearing without good reason, a further date is set. If the appellant does not attend, the appeal is considered on papers alone.
5. Where appropriate, and with the agreement of the appellant, the appeal hearing **CAN** be conducted via Skype or another secure communications facility. In such circumstances, those attending **SHALL** ensure the appropriate levels of security and privacy are in place for the duration of the hearing.
6. At the appeal hearing, the appellant **MAY** be accompanied by a work colleague from their respective organisation, who may be a trade union representative. Their role is confined to helping the appellant present their representations. They **SHALL NOT** answer questions directly on the appellant's behalf. Formal legal representation is not permitted. If there are any special requirements that the appeal officer needs to be aware of, this **SHOULD** be drawn to their attention in advance of the hearing so that necessary arrangements can be made.

7. The appellant **SHOULD** be provided with a written record of the hearing within 5 working days of the hearing taking place, to allow for their comments and to confirm or dispute the accuracy of the record. In the case of a dispute, both records should be retained.
8. If the appeal officer requires any further information during the appeals process, they **CAN** request this from either party at any time.
9. The appeal officer provides a report and recommendation to the Permanent Secretary within 15 working days of all enquiries being completed.
10. Where, for operational or management reasons, any of the previous timescales cannot be met, the appellant **SHOULD** be notified and, where possible, a revised timescale **SHOULD** be set. Similarly, where the appellant is unable to meet the timescales, the appeal officer **SHOULD** be notified and, where possible, a revised timescale **CAN** be agreed.

On receipt of the report, the Permanent Secretary is responsible for making the final decision. In reaching a final decision, they **SHOULD** consider:

- The statement of HMG personnel security and national security vetting policy, consideration of the interests of national security and the rights and interests of the individual.
- The merits of the original decision and the adequacy of the decision-making process.
- The appellant's grounds of appeal.

The Permanent Secretary informs the appellant of the outcome of their appeal in writing, giving the full reasons for their decision, related to the relevant facts, unless considerations of national security and confidentiality prohibit this. Where an appeal is rejected, the appellant is informed of their further right of external appeal to the Security Vetting Appeals Panel (SVAP). This concludes the internal appeal process.

External appeals

If an individual wishes to appeal against the outcome of the internal appeal, they **CAN** write to the Security Vetting Appeals Panel (SVAP), an independent advisory body which provides a final means of challenging a decision to refuse or withdraw a national security vetting clearance once an internal appeal has been dismissed. In such circumstances, the appellant is advised that if they wish to exercise a further right of appeal to SVAP, they **SHALL** notify the SVAP secretariat within 28 days of the decision of the internal appeal and provide contact details.

The SVAP is available to hear appeals from individuals in government departments and other organisations, or contractors' employees working for those departments and organisations, who have exhausted the internal appeals process and remain dissatisfied with the outcome. It is convened to hear cases as they arise, and consists of a Chairman and two members. The Chairman (and Deputy Chairman) is a senior member of the judiciary.

The SSA **MIGHT** be required to attend the SVAP hearing as well as the appeal officer.

The SVAP makes recommendations to the Head of Organisation in the light of its findings. It can recommend either:

- That the decision to refuse or withdraw security clearance **SHOULD** stand.
- That security clearance should be granted or restored.

The SVAP **CAN** also comment on the vetting procedures and the adequacy of the internal appeals process and make recommendations. The Permanent Secretary takes the final decision on whether to accept any recommendations to grant or restore a security clearance. Depending on the SVAP's findings, which are not binding, the Permanent Secretary **MIGHT** choose to consult with Cluster 2 Security Unit regarding next steps.

Annex B: Internal appeal form following refusal or withdrawal of security clearance

The Internal Appeal Form is available for download [here](#).

Who should complete this form?

This form should be completed by individuals engaged in work for the MoJ who:

1. Have had their security clearance refused or withdrawn; and
2. Have a right to appeal this decision.

Where should the form be sent?

If you are not sure that you have a right to appeal, refer to the Vetting Appeals Guidance.

Send completed forms to the Permanent Secretary, at the address provided to you in the letter which formally notified that your security clearance was refused or withdrawn. Appeals submitted by a third party on your behalf are not accepted.

PART A: Your details

Surname:

Forename(s):

Date of Birth:

Your current home address:

Any temporary address:

Contact telephone number:

Email address (for correspondence):

Department / Organisation:

Job title:

Please confirm you are content to receive correspondence by email at the email address you have provided here:

YES / NO

If no, please let us know where you would like correspondence sent?

Are you appealing against refusal or withdrawal of your security clearance?

YES / NO

If yes, what levels of security clearance were refused or withdrawn?

Do you wish to present your case in person at an appeal hearing?

YES / NO

Do you wish to be accompanied at the hearing by a member of staff or TUS representative?

YES / NO

If yes, please provide details of the individual who will accompany you:

PART B: Details of your appeal

For your appeal, you **SHOULD** provide a full rationale, with supporting facts if necessary, and include any information or documentation that **MIGHT** assist your appeal. Typically, an appeal submission **MIGHT** include information that was not previously available when the original clearance decision was made, where this information is materially relevant to your case. Use a continuation sheet if necessary.

PART C: Declaration

I declare the information given here is true and complete to the best of my knowledge and belief.

Signature of appellant:

Annex C: Framework of staff legal obligations in relation to HMG and Home Office material

Official Secrets Act

The Home Office **SHALL** adhere to the Official Secrets Act 1989 which came into force in 1990. It replaced section 2 of the Official Secrets Act 1911, under which it was a criminal offence to disclose any official information without lawful authority. Under the 1989 act, it is an offence to disclose official information. The act applies to:

- Crown servants, including Government ministers.
- Civil servants, including members of the Diplomatic Service.
- Members of the armed forces.
- The police.
- Government contractors, including anyone who is not a Crown servant but who provides or is employed in the provision of goods or services for the purposes of a minister.

Data Protection Act 2018 and UK General Data Protection Regulations

The handling of personal data must comply with UK Data Protection legislation. Departments and agencies should also have regard to UK Data Protection legislation, including any relevant exemptions, when sharing personal data with other departments and agencies or pursuant to international agreements.

Freedom of Information Act 2000

Classification markings can assist in assessing whether exemptions to the Freedom of Information Act 2000 (FOI) may apply. However, each FOI request **SHALL** be considered on its own merits as the classification is not a justifiable reason for exemption. It is therefore important that staff (including contractors) who handle, or are likely to handle sensitive assets, understand fully the impact of such legislation and how it relates to their role.

Public Records Act 1967

Records selected for preservation may be retained under Section 3(4) of the 1958 Act or closed under an exemption provided by the Freedom of Information Act 2000. Decisions over retention or closure are driven by perception of residual sensitivities at the time that release is being contemplated.

Contact details

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

Security vetting assessment of need

This form should be completed by a line manager or contract manager. Completion of this form allows Ministry of Justice (MoJ) Group Security to determine the correct level of National Security Clearance.

The assessment of need document is available [here](#).

Contact details

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

During employment

Ongoing Personnel Security

Security clearance is a snap-shot of an individual at the time they make their application. Therefore, it is essential that employees are proactively managed using effective ongoing personnel management processes.

When staff are inducted, they are advised of their security responsibilities. Line managers also have a key role in ensuring the security of the department, including personnel security of the people they manage. This is best achieved by following the guidance in this document.

Line Manager Responsibilities

- Brief your staff, including contractors, on local and departmental security arrangements and policies as part of their induction.
- Get to know your staff, including contractors who might only be employed for a temporary basis. This is so you can recognise any changes in their behaviour which might impact on the security of the organisation.
- Do not ignore any concerns you have for fear of not knowing what to do. Refer to the information in this guidance for further details.
- Where appropriate, deal with any concerns by talking to the individual, your manager, or HR.
- Create a positive climate in which security is given priority, and individuals are encouraged to discuss any concerns before they become security problems.
- Be a good role model for all your staff, and display good security behaviours.
- Remind all staff with security clearance (CTC, SC, or DV), that they **SHALL** [report changes in personal circumstances](#).
- Remind all staff that they **SHALL** notify the [security team](#) if they are travelling to certain countries referred to in the [Accessing Ministry of Justice \(MoJ\) IT systems overseas](#) guidance.
- Ensure you are aware of any relevant caveats, or aftercare measures, for staff with security clearance (CTC, SC, or DV), or other security guidance relating to your staff or contractors. Where relevant, make sure your successor is made aware of these requirements if or when you leave your post.

While holders of NSV clearance **SHALL** be aware of their responsibilities, as a manager you **SHOULD** be aware of these points:

- Holders of CTC, SC, and DV are expected to maintain the highest levels of personal integrity, honesty and discretion. They **SHOULD NOT** place themselves in positions where they could be open to compromise, pressure, or improper influence.
- Notwithstanding any set duration, security clearances **CAN** be reviewed at any point if there is a relevant change of circumstances, or new issues come to light.
- Holders **SHOULD** be aware of when their clearance expires, and apply to renew in time.
- Holders **SHOULD** adhere to Ministry of Justice (MoJ) [on-line social media policy](#). Holders **SHOULD NOT** publish their security clearance on-line, including on social networking sites.

Dealing with concerns

During your time as a line manager, you might notice unusual behaviours in some of your staff; they might behave out of character. It could be that someone else reports their unusual behaviour to you. It is your responsibility to engage with that individual promptly, and address any concerns that you have, or that are brought to your attention. Addressing areas of concern early on can prevent potentially damaging behaviour.

When speaking to an individual, remember:

- Your role as a line manager encompasses security, which means there is a duty of care not just to the individual but also the wider team.
- Vetted individuals **SHOULD** be encouraged to approach their line manager to discuss issues of concern. Early discussions allow appropriate action to be taken, and for support to be provided where appropriate.
- Dips in performance or changes in attitude might be an indication that staff have a wider problem or concern. Do not make assumptions, but do think about mitigations and support to prevent potential security implications.
- Do not put off talking to an individual for fear of not knowing what to do or say.
- Unusual behaviour might be nothing to do with security issues, but might be for several reasons. Listen to the person, and, if possible, offer your support. It might be appropriate to refer them to a [support group available within](#) the MoJ.

Note: For more information, refer to the MoJ [Support and wellbeing](#) resources.

Managing security clearances requires active conversations between managers and individuals throughout the year, and prompt reporting of any issues of concern: [Reporting personal circumstance changes](#). Whilst there are formal renewal periods, clearances may be reviewed, suspended, or withdrawn at any time.

Managing contractors or consultants

As with any staff, managers are responsible for ensuring that the appointment of contractors or consultants meets MoJ security requirements, and that ongoing personnel security is maintained throughout their stay in the MoJ.

Managing a contractor or consultant is normally similar to managing a permanent member of staff. However, given the sometimes transient and flexible nature of a contractor or consultant's work pattern, managers **SHALL** pay more attention to them in terms of recruiting and security responsibilities.

There is a good chance that a contractor is not familiar with the MoJ's security procedures and practices, or even the MoJ's [Intranet site](#). They might not be aware of the threats faced by HMG, or the specific governmental department for which they work. Advise them that Government work **SHALL NOT** normally be carried out on [personal IT devices](#).

Summary

- Prior to their appointment, contractors or consultants **SHALL** be security cleared to the appropriate level for their specific role.
- Only a permanent employee (civil servant) can sponsor a security clearance.
- Only a permanent employee (civil servant) can act as a sponsor for the issuing of a building pass. Appropriate security clearance **SHALL** be obtained before sponsoring an application for a building pass.
- "Escorted" visitor passes are exclusively for the use of visitors. Contractors or consultants paid by the MoJ are not visitors, and **SHALL NOT** be issued with a visitor pass. They **SHALL** be cleared in advance of them starting work, and issued with the correct pass.
- When transferring security clearance from another Government department, [Cluster 2 Security Unit](#) **SHALL** confirm if the security clearance is valid and current. If not, a new security clearance application **SHALL** be started.
- Holders of CTC, SC, or DV **SHALL** [report changes in personal circumstances](#).
- Remind all staff that they **SHALL** [refer to the travel abroad guidance](#).
- Ensure contractors, like all staff, are aware of [MoJ security policies](#), and check their understanding. Make sure they are briefed on good security behaviours, and act as a role model.
- Ensure they are aware of the MoJ [on-line social media](#) guidance and understand the need to avoid publishing their security clearance on social media.
- Create a positive environment in which security is given priority, and individuals are encouraged to discuss concerns before they become serious problems.
- As part of your role, you **SHOULD** seek to get to know your contractor or consultant, and discuss any behavioural changes.
- Although contractors often have a short contract, that might or might not be renewed, they are still given security clearance for a number of years: 5 years for CTC, and 7 years for SC and DV. If their contract period is less than the renewal cycle, then you **SHALL** notify [your local National Security Vetting Contact \(NSVC\)](#) when the contractor leaves, so that their security clearance can be terminated.

Contact details

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

Personnel risk assessment

This guidance is written for departmental and line managers that manage staff. These staff may include, but are not limited to: permanent employees, individuals on attachment or secondment, contractors, consultants, agency and temporary staff.

Personnel security risk assessment focuses on employees and contractors, their access to Ministry of Justice (MoJ) assets, and the risks they could pose. This is set against the adequacy of existing countermeasures. This risk assessment is crucial in helping you communicate to senior managers the risks to which the organisation is exposed.

This guidance aims to help risk management practitioners to:

- Conduct personnel security risk assessments in a robust and transparent way.

- Prioritise the insider risks to an organisation.
- Evaluate existing countermeasures, and identify appropriate countermeasures to mitigate those risks.
- Allocate security resources, which might be personnel, physical or informational in nature, in a way which is cost-effective and proportionate to the risk posed.

Personnel security

Personnel security is a system of policies and procedures that seek to manage the risk of people exploiting, or having the intention to exploit, their legitimate access to the organisation's assets for unauthorised purposes. Those who seek to exploit their legitimate access to systems and data are called "insiders" and they pose an "Insider Risk".

A person who causes harm to the MoJ might have access to assets for one day a month, or every working day. They might be a permanent member of staff, or a contractor. Their access might be in a traditional office, or site setting, or remote. This guidance covers all people who are given legitimate access to MoJ assets and premises.

The guidance for Personnel Risk is not prescriptive. It provides a framework to work with but, to be successful, it requires the MoJ to bring together the right people and information. The more you put into this process, the more worthwhile and useful the results will be.

Risk management

Risk management is the foundation of the personnel security management process and is a continuous cycle of:

- Identification: identify the risks to the role.
- Risk assessment: assess the risks to the organisation and its assets in terms of the likelihood of a threat taking place, and the impact that such an event might have.
- Implementation: identify and implement security measures to reduce the likelihood and impact of the threat to an acceptable level, bearing in mind that risk can not be completely removed.
- Evaluation: assess the effectiveness of the countermeasures and identifying corrective actions.



Figure 1: Risk Management Cycle

The methodology defines risk as the product of two factors:

- The likelihood of an event occurring.
- The impact that the event would have.

When each of these factors has been evaluated, they are combined and this provides the overall measure of risk.

The cyclical nature of the process ensures that the implementation and evaluation stages are reviewed each time a risk assessment is repeated.

Much of the value of the risk management process comes from the systematic exploration of threats, opportunities, and countermeasures, through engagement with other parties. These differ between departments but can include HR, security, senior management, information specialists, and other technical specialists as appropriate.

The Risk Management process

The MoJ uses the risk management process developed by the Centre for Protection of National Infrastructure (CPNI). A copy of the CPNI's guide can be found [here](#).

Managers and other risk management professionals **SHALL** follow the process set out in the guide, and maintain detailed records. These **SHOULD** be made available when requested by Audit, Group Security, or HR.

Downloads

- [Ongoing personnel security: A good practice guide.](#)
- [Personnel security risk assessment.](#)

Contact details

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

Reporting personal circumstance changes

Reporting changes in personal circumstances for staff with National Security Vetting.

National Security Vetting decisions are made based on information available at the point of clearance. However, people's lives change over the course of a clearance. It is important that relevant changes are reported so that any risks can be assessed and managed.

To maintain your security clearance, it is your responsibility to declare relevant changes in your personal circumstances to VettingAftercare@cluster2security.gov.uk. Failure to report relevant changes could result in withdrawal of clearance.

You **SHALL** contact VettingAftercare@cluster2security.gov.uk if there is any significant change in your personal circumstances and **SHALL** alert your line manager or contact the VettingAftercare@cluster2security.gov.uk directly if you become aware of any other issue which might increase your security vulnerability.

Please contact VettingAftercare@cluster2security.gov.uk if you have any of the following changes to your personal circumstances.

Personal circumstances

- Change of name.
- Change of marital status.
- Change of nationality.
- New cohabitant, for example new partner (CTC, SC, and DV), or co-residents (DV only).

Personal finances

- Any major new financial changes for example new income, significant change of mortgage, or negative financial impact of divorce or separation.
- Any major capital gain over £5,000, for example gifts, an inheritance, or a National Lottery win.
- Any other significant financial change, for example debt, loss of earnings causing a negative effect or bankruptcy.
- Regular use of payday loans.

Health, personal problems and aspects of lifestyle

- Domestic, marital, or other events causing significant distress.
- Dependence upon alcohol, use of illegal drugs, substance abuse, or misuse of prescription drugs.
- Any addiction, for example gambling or spending, or other physical, or psychological dependence.
- Any other aspect of your lifestyle you would seek to keep a secret from others which could make you vulnerable to pressure or blackmail if discovered.

Legal matters and involvement with the police

- Arrests, pending prosecutions, convictions, formal police cautions, or police enquiries, which might lead to prosecution, except for parking and minor traffic offences.
- Interviews with the police as a suspect in connection with any criminal investigation.
- Likely or actual involvement in civil legal proceedings, either as a defendant or plaintiff, for example subject of a County Court judgement.

Links with extremist or secretive organisations

- Any political, religious, or other organisation holding extreme views, for example advocating violence, or rejecting parliamentary democracy.
- Any organisation requiring exceptional or exclusive loyalty.
- Any organisation which is unusually secretive about its affairs.
- Any organisation whose aims, beliefs, or activities might conflict with working for Her Majesty's Government.

Overseas links or inappropriate associations

- Close relationship or connection with someone from a country of security significance.
- Financial or business links to a country of security interest.
- Associations with individuals that could be in conflict with your role, and make you vulnerable to pressure.

This list is not exhaustive, so contact us if you require advice, or are unsure about what to declare. Please also report any other changes that might alter an answer provided in the security questionnaire at the time of clearance, or the financial questionnaire, if you completed one.

Change of personal circumstance questionnaire

In some cases where further checks need to be conducted, you are asked to complete a Change of Personal Circumstance questionnaire. You are asked to complete this form if you hold a security clearance (Developed Vetting (DV), Security Check (SC), or Counter-Terrorist Check (CTC)), under the following circumstances:

- When you get married, enter a civil partnership, or start living with a partner as a couple.
- If you hold a DV clearance, when a new co-resident (anyone aged 18 or over for example lodgers, flat-mates, etc.) begins living with you in shared accommodation.

Changes in circumstances for another member of SC cleared staff

If you become aware of a change in circumstance for another member of security cleared staff, you **SHOULD** remind them of their responsibility to report this to VettingAftercare@cluster2security.gov.uk.

You must alert your line manager or VettingAftercare@cluster2security.gov.uk if you become aware of any other issues which might increase your security vulnerability, or the security vulnerability of a security cleared colleague. All staff **SHOULD** be mindful of circumstances and behaviours that might render staff susceptible to pressure, or improper influence, or could otherwise indicate unreliability.

Other obvious changes in circumstances, aside from those already listed previously, are:

- Serious financial problems.
- Substance and drug abuse.
- Alcohol abuse.
- Illegal or injudicious behaviour, including when living or travelling overseas.
- Compulsive gambling.
- Involvement with extreme political groups or inappropriate associations.
- Sexual behaviour is a security concern if it involves a criminal activity, indicates a personality or emotional disorder, subjects the individual to coercion, exploitation, or duress, or reflects lack of judgement or discretion. Sexual orientation or preference are not in themselves disqualifying factors, and are not used as a basis for clearance decisions.

All reports are treated in strict confidence. It is always better to alert a line manager or contact VettingAftercare@cluster2security.gov.uk directly, rather than to ignore an issue or take no action.

Contact details

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

Training and Education

Overview

This information applies to anyone and everyone working for, or with, the Ministry of Justice (MoJ).

The MoJ's Information Security awareness programme plays an essential part in maintaining security. It informs all MoJ staff of:

- Their duties with regard to security.
- Their responsibilities to protect the assets (information, equipment, people and buildings) they have access to and use.
- The importance of reporting any actual or suspected security incidents.

Requirements

All staff starting or returning to work within the MoJ **SHALL** receive mandatory security training.

The objective is to ensure that all new and current staff members are aware of their security responsibilities whilst working at the MoJ.

Full details of the mandatory training are provided in the Joiner, Mover, and Leaver pages on the MoJ [Intranet](#).

In summary, as a minimum everyone **SHALL**:

- Have taken and completed an MoJ Security [induction](#).
- Have completed the [Civil Service Learning](#) course on "Responsible for Information (RfI)", or an approved equivalent.

Normally, this training **SHALL** be completed successfully before accessing MoJ information, resources, or assets.

Further information

More details are provided to staff on the MoJ Intranet, <https://intranet.justice.gov.uk/>.

Contact details

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

Voluntary drug testing policy

Scope

This policy covers access to a range of government assets at risk from a wide range of national security threats. These threats may be related to terrorism, espionage, sabotage, or serious organised crime. Vulnerabilities may also arise from disaffected employees (known as "insiders") who could seek to exploit their level of access.

This policy **SHOULD** be read in conjunction with the [Voluntary Drug Testing Policy Procedures](#).

Purpose

Substance misuse threatens the efficiency and delivery of business. It might impair judgement and affect an employee's ability to carry out their role and responsibilities effectively and to the standard expected from HMG and the public.

Additionally, it might make an individual vulnerable by leaving them open to pressure, inducement, or blackmail. It might also affect their suitability to continue to hold security clearance.

This policy sets out the Ministry of Justice (MoJ) approach to voluntary drug testing which is used as a risk management tool for personnel security. It helps identify potential risks and vulnerabilities to national security and allows them to be managed appropriately and proportionately.

Specifically, it seeks to:

- Minimise the likelihood of existing employees becoming a security concern.

- Implement security measures in a way that is proportionate to the risk.

Government Functional Standard Outcomes

The [Government Functional Standard - GovS 007: Security](#) states personnel assurance is fundamental to good security. It demands that Government organisations delivers the appropriate combination of recruitment checks, vetting, and on-going personnel security management. This allows them to be assured about their people and to mitigate risks from well-placed insiders.

Policy Statement

To achieve this security outcome, the following **SHALL** be followed by the MoJ.

- Determine the need for voluntary drug testing using a threat and risk management approach, based on evidence supplied throughout the National Security Vetting (NSV) process.
- Individuals **SHOULD** co-operate fully with any request to provide a voluntary sample collection for drug testing.
- Confirmation of test results, and any subsequent decision making made, **SHALL** be held on the individual's vetting file, and stored in accordance with the organisation's retention periods.
- Test results **SHALL NOT** be used for any other purpose than deciding suitability to hold NSV. Exceptions to this include legal obligations (for example Court order, or Police warrant), or the transfer of records to another Vetting Authority, as part of clearance confirmation procedures, or where there is an overriding corporate duty of care to the vetting subject.
- Any new information or concerns affecting the reliability of an individual **SHALL** be reported to, and dealt with by, [MoJ Group Security](#), in conjunction with the Senior Security Advisor.

Voluntary drug testing policy procedures

Introduction

The Cluster 2 Security Unit (C2SU) forms part of the Transforming Government Security programme which aims to standardise and strengthen operational security across Government.

Cluster 2 is one of four cross-Government Security Clusters which delivers operational security services to the following Government organisations:

- Home Office
- DEFRA
- Department for Education
- Department for Transport
- Ministry of Justice (MoJ)
- Ministry for Housing, Communities, and Local Government

The MoJ Senior Security Advisor (SSA) is responsible for the overall management of security and for ensuring that the Cluster services and policies provided meet Government and organisational aims for improved security in Government.

If you have any queries about this information, contact [MoJ Group Security](#).

Procedures

These policy procedures support and underpin the [Voluntary Drug Testing Policy](#). Unless otherwise noted, these procedures **SHALL** be complied with fully.

Aftercare arrangements: Use of Voluntary Drug Testing

A security clearance requires ongoing review. A voluntary drugs test is one of a range of vetting aftercare arrangements which provides assurance and confirms that staff are suitable for ongoing access to sensitive government information and assets. Drug testing is a voluntary process which enables security clearances to be assessed and granted in cases where they would ordinarily be refused.

Voluntary drug testing is used when illegal drug use is admitted to during the vetting process.

C2SU decide on a case-by-case basis whether drug testing is necessary. C2SU also identify any potential security risks to Government assets in consultation with the MoJ Senior Security Advisor. In any event, the individual must commit to not using any type of illegal drugs during any period of employment with the MoJ.

Drug testing arrangements

C2SU set a timeframe in which an individual will be periodically tested for a panel of illegal drugs by an accredited and approved drug testing provider.

Disclosure of personal information

Personal information needs to be disclosed to the approved drug testing provider to support the administration of the drug testing process. By agreeing to take part in the voluntary drug test, the individual is subsequently consenting to the following personal information being provided:

- Full name.
- Date of birth.
- Place of work (for example, MoJ).
- Declaration of illegal drug use both historic and current (including type of drug(s), frequency, and quantity).
- Declaration of controlled substances both historic and current (for example, prescription medications).
- Other medical history required to help safely facilitate the drug testing process.

This information is used only for the purposes of facilitating the drug testing process.

Sample collection

The primary method for the sample collection is a hair sample. However, in some circumstances other alternative methods, such as a urine sample, may be used for drug testing analysis. At each drug test an alternative hair or urine sample is taken to allow for independent re-testing, if required (for example if a test result is inconclusive or further evidential testing is required).

The individual is expected to co-operate fully with any request to provide a sample collection. If the initial request cannot be met due to availability issues, such as pre-arranged annual leave commitments, the individual must arrange as soon as possible with the C2SU's drug testing provider, and no later than five working days after the unavailable period, to provide a sample collection for drug testing analysis.

If, due to a change of circumstances beyond the individual's control, they are unable to attend the scheduled appointment, they must give advanced notice (minimum of 24 hours) and reason(s) for non-attendance to C2SU and the drug testing provider. The appointment must be rescheduled within seven days of the original appointment date.

Failure to either provide advanced notice to C2SU and the drug testing provider, or reschedule the original appointment date within the set timeframe, is interpreted as the individual's unilateral withdrawal from the vetting aftercare arrangements, and could lead to withdrawal of the security clearance.

Failure to co-operate with any part of the drugs testing process, or if C2SU has reason to believe that deliberate attempts by the individual are being made to delay, frustrate, or circumvent the process, is interpreted as the individual's unilateral withdrawal from the national security vetting aftercare arrangements and could lead to the withdrawal of the security clearance.

Raising concerns

Any concerns about the sample collection process, or about the approved drug testing provider, must be raised with C2SU at once and in any event prior to receiving confirmation of drug testing results. C2SU investigates any concerns raised with the approved drug testing provider.

Confirmation of test results

Confirmation of test results is provided in full to the individual, and shared in their entirety with the Cluster 2 Aftercare Security Unit.

Any positive trace of illegal drugs is grounds for assessing the individual's suitability to hold security clearance. The level of security clearance withdrawn is decided by C2SU on a case-by-case basis.

Confirmation of test results, and any subsequent decision making made by C2SU, is held on the individual's vetting file and stored in accordance with C2SU retention periods.

The test results are not be used for any purpose other than deciding on suitability to hold national security vetting. Exceptions to this include legal obligations (for example court order or police warrant), or the transfer of records to another Vetting Authority as part of clearance confirmation procedures, or where there is an overriding corporate duty of care to the vetting subject.

Self-reporting

Following the Cluster 2 department's Drugs and Alcohol Substance Policy, or equivalent, individuals misusing substances are encouraged to discuss this with their line manager and urged to seek expert help and advice at the earliest opportunity.

Additionally, holders of national security vetting clearance at all levels are expected to show the highest level of honesty, integrity, transparency, openness, and frankness in sharing personal information (including lifestyle habits, and changes to them) of security relevance, or when engaging with C2SU. Dishonesty and intent to mislead or conceal is viewed seriously and influences whether the clearance is kept.

All information shared with C2SU is treated in confidence. Support is provided where possible.

Self-reporting of any drug misuse is not necessarily considered as automatic grounds for the withdrawal of security clearance. C2SU assess everyone on a case-by-case basis. However, failure to self-report drug misuse which later comes to light via drug testing, or any other means, is likely to lead to security clearance being withdrawn.

The following contributing factors are considered by C2SU. This is not an exhaustive list:

- The type and quantity of illegal drug usage.
- Previous history of the misuse of illegal drugs.
- How long since the previous declaration of illegal drugs use.
- How the illegal substances were acquired.
- The environment in which the illegal drug use took place.

C2SU assess an individual's suitability to continue to hold security clearance by deciding the level of risk they have of being susceptible to pressure or improper influence, or indicate unreliability, because of their actions. The principles around national security vetting focus specifically on the threats posed to UK national security (for example terrorism, espionage, or other actions that would threaten the UK). The threats and any subsequent risks to the business might differ, so they are assessed and managed by locally produced business-related policy and procedures.

Appealing decisions of withdrawing security clearance

If a security clearance is withdrawn following a positive test result, the appeal rights and processes are the same as for withdrawal or refusal of national security vetting clearance for any other reason. Any appeal is dealt with following the terms of the Security Clearance Appeals Procedure. These state that Right of Appeal applies to those falling under these criteria:

- Permanent members of MoJ staff.
- Current contractors or other non-permanent staff, already engaged in MoJ work.
- Current permanent members of staff of other government departments and organisations who have applied for or transferred a security clearance with the MoJ.
- Current contractors already engaged on government work in other departments and organisations who have applied for or transferred a security clearance with the MoJ.

There is no Right of Appeal for individuals on recruitment to the Civil Service seeking employment or contractual work with the MoJ. For further information on the Security Clearance Appeals Procedure, contact Group Security: mojgroupsecurity@justice.gov.uk.

Appealing a positive drug test

Any disputed drug test **SHALL** be appealed to C2SU, in writing, within five days of receiving confirmation of a test result.

An appeal **SHALL** detail the reason or reasons why the positive result is being disputed. This information **SHALL** be shared with the approved drug testing provider and the positive test results **SHALL** be subject to further scientific expert analysis to decide the probability of the positive test result being incorrect. The results of any secondary testing **SHALL** be treated as final.

Review of drug testing arrangements

The requirement for drug testing individual cases **SHALL** be subject to ongoing review, on a case-by-case basis, by C2SU. The individual **SHALL** be formally notified by C2SU if this aftercare arrangement is withdrawn.

Termination and change of employment

End or change of employment

Managers must ensure that all employees, contractors and third-party users return all assets within their possession and that all access rights (including building passes, access to buildings, IT systems, applications and directories) are removed at the point of termination or change of employment.

If the leaver has security clearance, managers should contact the [Cluster 2 Security Unit](#) 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.

Leavers with NSC and NSVCs

This information applies to people leaving the Ministry of Justice (MoJ), who have National Security Vetting (NSV), or who are National Security Vetting Contacts (NSVCs).

Staff or contractors that hold clearance of any level **SHALL** attend an exit interview with their manager before they leave the MoJ. Although these interviews are available for all staff, they are compulsory for those with Counter Terrorist Clearance (CTC) or Security Check (SC).

If the leaver holds Developed Vetting (DV) or SC enhanced level, and has been STRAP inducted, they **SHALL** attend a mandatory STRAP debriefing interview with [Cluster 2 STRAP team](#). They **SHALL** also sign a confidentiality agreement and a "Declaration of Cessation of TOP SECRET STRAP Access".

NSVCs who leave

The post of National Security Vetting Contact (NSVC) **SHOULD NOT** be left empty. NSVCs **SHOULD** work with [MoJ Group Security](#) to ensure that a replacement has been selected, and trained, to take over once they have left.

Manager responsibilities

When a member of staff with clearance leaves their department, the manager **SHALL** inform their NSVC, so that the NSVC can update their records and remove the staff member from the list of cleared personnel. The NSVC passes the leaver's details on to [Cluster 2 Security Unit](#). Managers **SHOULD** also use this as an opportunity to take another look at the role, and confirm whether it still needs clearance and, if it does, to what level. The NSVC can advise managers on this analysis.

Downloads

- [National Security Vetting Contact Guide.](#)
- [National Security Vetting Contact Register.](#)
- [National Security Vetting Assessment of Need.](#)

Related information

- [End or change employment.](#)

Contact details

For any further questions relating to group security matters, contact: mojgroupsecurity@justice.gov.uk. For general security questions or concerns, 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.

Acceptable use can also vary according to context. For example, checking sensitive personal details might be perfectly normal within a secured office, but is not acceptable in a public space where anyone else might access those details.

Unacceptable use of MoJ IT

Unacceptable use of IT prevents you or your colleagues from doing work, or is unlawful or illegal, or does not take the context into account.

There are many unacceptable uses of IT, making it impossible to provide a complete list. Examples of things to avoid include:

- Deliberately or accidentally sharing resources or information, such as passwords, with people who are not supposed to have them.
- Using resources without permission.
- Storing sensitive information where it could easily be lost or stolen.
- Using unapproved tools or processes to store sensitive information, such as passwords or credit card details.
- Using your work email address for personal tasks.
- Using your personal devices or your personal email address for work tasks.
- Excessive private use during working time.
- Installing unlicensed or unauthorised software.
- Redirecting print jobs from MoJ printers to a personal printer.
- Sending your work material to your personal devices or your personal email accounts. (It is of course acceptable and necessary from time-to-time to send work material to someone else's email address when they are directly involved with that work, for example someone in the Office of the Public Guardian (OPG) emailing someone regarding Lasting Power of Attorney (LPA).)

Why unacceptable use is a problem

Unacceptable use of IT might affect the MoJ in several ways, such as:

- Bad publicity or embarrassment.
- Increased or unexpected costs or delays.
- Civil or legal action.
- Reduced efficiency and effectiveness.

Unacceptable use might also affect you, too:

- Suspension of access, so that you cannot do your work.
- Disciplinary proceedings, up to and including dismissal.
- Termination of contract for contractors and agency staff.

Keeping control

You are responsible for protecting your MoJ IT resources. This includes keeping your usernames and passwords safe and secure.

It also means looking after MoJ equipment, especially when working away from MoJ locations. You are responsible for protecting MoJ equipment issued to you. Any theft of MoJ equipment, or deliberate or wilful damage to MoJ equipment, should normally be [reported](#) to the Police and to the IT Service Desk.

Note: You should normally report instances of theft or damage to authorities as indicated. However, there might be additional circumstances which mean a sensitive handling of the situation is appropriate. It is acceptable to consider the context of the situation when making a report. Ensure you can justify your actions. In cases of uncertainty, don't hesitate to ask your line manager, or other responsible authority for advice.

While you might be careful about acceptable use of MoJ IT, there are still risks from [malware](#), [ransomware](#), or [phishing](#) attacks.

If you get an email from anyone or anywhere that you are not sure about, remember:

- Don't open any attachments.
- Don't click on any links in the email.

If there is any doubt, or you are worried that the [email might be malicious](#) or inappropriate, [report it immediately](#) as an IT security incident.

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.

Introduction

MoJ IT systems and services are first and foremost provided to support the delivery of the MoJ's business services. To achieve this, most MoJ users are provided with an appropriate general purpose computer environment, and access to services and communication tools such as email and the Internet.

This policy outlines the acceptable use of MoJ IT systems and services, and the expectations that the MoJ has on its staff when accessing or using those systems or services.

Scope

This policy covers all Users (including contractors and agency staff) who use MoJ IT systems or services.

Failure to adhere to this policy **MIGHT** result in:

- Suspension of access to MoJ IT systems and services.
- For MoJ employees, disciplinary proceedings up to and including dismissal.
- For others with access to MoJ IT systems and services, including specifically contractors and agency staff, termination of contract.

POL . ITAUP . 001: All Users **SHALL** be made aware of the Acceptable Use Policy (this document), and provided with security awareness training which covers this policy.

POL . ITAUP . 002: All Users **SHALL** undergo refresher security awareness training covering this policy, every 12 months.

Protection of assets

It is paramount that all Users protect the confidentiality of information held on, processed, and transmitted by MoJ IT systems. All Users have a role in protecting the information assets which are under their control, or that they have access to.

MoJ IT systems have been designed to protect the confidentiality of the data held on them. However, maintaining this requires the application of, and adherence to, a clear set of operating procedures by all Users. These are collectively known as Security Operating Procedures (SyOPs).

It is important that all Users of an IT system, including support and system administrative Users, are familiar with these SyOPs, and are provided with the appropriate training.

POL . ITAUP . 003: All IT systems **SHALL** have, and maintain, a set of Security Operating Procedures (SyOPs). For systems undergoing an assurance process, these SyOPs **SHALL** be included as part of the assurance.

POL . ITAUP . 004: All Users of an IT system, including support and system administrative staff, **SHALL** read the applicable SyOPs, and **SHALL** acknowledge that they have both read and understood the SyOPs before being granted access. A record **SHALL** be kept of a User being granted access, and made available for review during assurance, or upon authorised request.

POL . ITAUP . 005: All Users **SHALL** be made aware that non-conformance to the system SyOPs constitutes a breach of the MoJ [IT Security Policy](#), and **MIGHT** result in disciplinary action.

POL . ITAUP . 006: Any change to an IT system's SyOPs **SHALL** be approved through an assured change control process, before the change is made.

POL . ITAUP . 007: Any request to perform an action on an IT system which contravenes its SyOPs **SHALL** be approved by the [Security team](#) before the action is taken.

For most Users, access to MoJ IT systems and information held on them is through a desktop device, a laptop, or a mobile or remote device. These devices have the capacity to store large amounts of potentially sensitive information assets. It is important that Users follow Information Management processes and handling guidelines to ensure information is stored and accessed appropriately. Further information on information handling is provided in the [Information Classification and Handling Policy](#).

General Security Operating Procedures (SyOPs)

The policy refers to a key set of general SyOPs, as follows:

- [Remote Working](#).

To minimise the number of SyOPs in circulation and standardise procedures, the SyOPs listed previously act as the primary set, which individual IT systems are expected to conform to, in terms of their own SyOPs. Any deviations or additions are dependent upon approval through the assurance process.

POL.ITAUP.008: All IT systems **SHALL** have documented SyOPs which comply with the general SyOPs [listed in this policy](#). Any deviations or additions **SHALL** be recorded in separate SyOPs which form an addendum to one of the SyOPs [listed](#).

Note: An IT system **MAY** make use of, in their entirety, one or more of the SyOPs listed in this policy if the procedures of that IT system do not deviate from those described in the general SyOPs.

Removable Media

Removable storage media include devices such as USB memory sticks, writeable CDs or DVDs, and external drives. These devices **MIGHT** contain large amounts of protectively marked data, and so pose a significant risk to the confidentiality of the data they hold. As such, the MoJ controls the use of removable media through SyOPs, technical security controls, and by requiring movements of bulk data to be authorised.

POL.ITAUP.009: Any removable media device **SHALL** be approved by MoJ security, where that device is used to store protectively marked data. The type of device and associated SyOPs **SHALL** be approved by MoJ security before operational use.

POL.ITAUP.010: All Users **SHALL** ensure that all data stored on or transported by removable media is in accordance with the applicable system SyOPs.

POL.ITAUP.011: All Users **SHALL** seek approval from the [Security team](#) prior to any bulk transfer of protectively marked data using removable media. MoJ security advises on any technical and procedural requirements, such as data encryption and handling arrangements.

Passwords

A username and password combination is the primary access credential used for authenticating a User to MoJ systems, and authorising User access to information assets and services provided by that system. It is therefore important that Users keep their access credentials safe and secure.

POL.ITAUP.012: All Users **SHALL NOT** share or disclose any passwords with any other person.

POL.ITAUP.013: All Users **SHALL NOT**:

- Attempt to gain unauthorised access to another User's IT account.
- Attempt to use another Users access credentials to gain access to an MoJ system.
- Attempt to access information for which they do not have a 'need-to-know'.
- Use the same password on more than one MoJ system.

Legal and regulatory requirements

There are a number of legal and regulatory requirements that the MoJ must comply with. These obligations are in addition to HMG security policy, as expressed in the [HMG Security Policy Framework](#).

POL.ITAUP.014: All Users **SHALL** be made aware of legal and regulatory requirements that they **SHALL** adhere to when accessing MoJ systems. These requirements **SHALL** be included as part of the SyOPs.

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 . 021: 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 Privacy Team](#), after which the transfer **MIGHT** be approved. A template for these documents can be requested from privacy@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 Privacy 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 Privacy Team](#).

The documents are as follows:

- Acceptable Use Protocol Commercial and Contract Management
- Acceptable Use Protocol Subject Access Requests
- Acceptable Use Protocol Storage of Personal Data
- Acceptable Use Protocol Data Subjects' Rights
- Acceptable Use Protocol Processing of People Data
- Acceptable Use Protocol Analytical Platform
- Acceptable Use Protocol Recording

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 Privacy 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/>

When to remove access and return assets

In a number of circumstances assets should be returned and access should be removed. This is where:

- The leave is longer in duration, and there is no business need or individual need for the user to keep assets and access. This should be considered for any leave more than 12 months in duration. This is likely to be for Career Breaks or Loans.
- The staff member has no means of securely storing the asset, for example locking it securely in their home.
- Staff members going on leave for less than 12 months may return their assets and have access removed if they choose to do so.
- Line managers are empowered to determine whether the staff member should keep assets and access, as long as there is appropriate business justification, and staff members are appropriately supported. For example, a communication mechanism for keeping in touch is agreed.
- If, during their leave, the staff member decides to end their employment (resign), their line manager is responsible for following the appropriate leaver's process with them. Refer to the Resignation section of the HR guidance and forms, with particular reference to the Leavers Checklist for Managers. This can be found at: <https://intranet.justice.gov.uk/guidance/hr/end-change-of-employment/resignation/>

How to remove access and return assets

- Access to systems and return of assets can be organised through the appropriate items in the [MoJ Technology Portal](#). Please refer to the Knowledge Base article on "Returning your MoJ laptop, accessories and mobile phones" for details. Removal of access to local systems should be arranged with local IT teams.

Note: When a Dom1 account is deactivated, its data is recoverable for up to 12 months. Refer to the Knowledge Base article on "How to Re-instate a Deactivated Email Account or Mailbox".

Contact details

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

Protect yourself online

There are five simple things we can all do to protect ourselves online:

1. Use a strong password to protect your laptop, computer and mobile devices. To choose a good password, follow [NCSC guidance](#).
2. Think before clicking on links or attachments within emails. By hovering your cursor over the link you can find the actual URL. If you are unsure if an email is genuine, [contact your IT or security team](#).
3. Do not use your work email address to register for accounts on websites for personal use. For example, a shopping website does not need your work email address. Using the wrong address could open up your work email account to spam and fraudulent emails. This in turn could harm your department's IT system.
4. Protect your online identity. Do not share sensitive information about your work on social media or online professional networks.
5. Do not disclose your level of vetting. If you share this information, you advertise what resources you have access to. This could make you a target for malicious individuals.

For more information, refer to the [Acceptable Use guidance](#).

Contact details

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

Information classification

Data Handling and Information Sharing Guide

This guide is designed to help protect Ministry of Justice (MoJ) information held on MoJ IT systems, by providing guidance on how it should be handled and shared in a safe and secure manner.

Overview

Introduction

The [Government Functional Standard - GovS 007: Security](#) identifies mandatory requirements about the value and classification of information assets. To comply with these requirements, the MoJ needs to ensure that:

Where information is shared for business purposes, departments and agencies **SHALL** ensure the receiving party understands the obligations and protects the assets appropriately.

and

All staff handling sensitive government assets are briefed about how legislation (particularly regarding Freedom of Information and Data Protection) specifically relates to their role, including the potential disciplinary or criminal penalties that may result from failure to comply with security policies. Appropriate management structures **SHALL** be in place to ensure the proper handling, control and (if appropriate) managed disclosure of sensitive assets.

The policy on data handling and information sharing is covered in the Information Classification and Handling Policy, whilst this document sets out the MoJ guidance sharing information within the MoJ and externally with other Government departments and 3rd parties.

Note: Other guidance might refer to information classified as being IL3 REST*. This is an older classification standard. In general, IL3 REST* is approximately equivalent to OFFICIAL with the SENSITIVE handling caveat, often written as OFFICIAL-SENSITIVE. While this approximate alignment might be helpful, you should always review classification where older terms are used, to ensure that the correct current classification is used.

Scope

This document provides guidance on handling or sharing information stored on MoJ IT systems, or exchanged electronically within the MoJ, or with external parties.

The MoJ [Security team](#) can help you with more guidance on the handling of protectively marked data.

This guide is split into three sections:

- [Handling data](#) on MoJ IT systems.
- [Information sharing](#).
- [Reporting data loss](#).

Note: This document provides guidance for handling and sharing of information and data up to and including OFFICIAL and OFFICIAL-SENSITIVE, or the older Impact Level (IL) 3. Where information attracts a high protective marking or IL, advice **SHALL** be sought from the MoJ [Security team](#) and the MoJ Chief Information Security Officer (CISO).

Handling data on MoJ IT systems

This section covers how data **SHALL** be handled on MoJ IT systems, this includes both:

- Data in transit.
- Data at rest.

For the purposes of this guide, the term "sensitive" data or information refers to data or information which attracts a handling caveat of **SENSITIVE**.

Ownership of information

All MoJ information is assigned an individual who has overall responsibility for the various handling aspects including:

- Registration.
- Labelling.
- Storage.
- Any transfers.
- Setting a retention period.
- Deleting, destroying or 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 solely on non-networked devices or 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.

Information sharing

General principles

Where there is a business need to transfer sensitive data, it **SHALL** be appropriately secured or encrypted using an approved mechanism prior to electronic transmission or export to removable media devices.

Transferring sensitive data with the appropriate security controls may be achieved by:

- Transmission over a secure network that is accredited to carry such data, either in clear (where this has been formally approved by Information Assurance and the IAO), or encrypted.
- Transmission over an unprotected network, employing encryption of sufficient strength to mitigate any communication security risks identified.
- Physical transportation of storage media using encryption of sufficient strength to mitigate the security risks associated with the information being transferred in addition to the physical and procedural measures required to protect the media itself.

Note: Only the minimum amount of sensitive data necessary to meet the business requirement should be transferred and not the entire data set.

The sender **SHALL** ensure that any data shared can be adequately secured by the recipient. The sensitivity of data **SHALL** never be downgraded in order to send it over inadequately protected channels, or to send it to a recipient who does not have an appropriate facility to protect it after it arrives.

Sharing sensitive information

MoJ staff, including contractors and agency staff, **SHALL** make sure they observe the following measures when sharing sensitive information:

- Check that all recipients are authorised and cleared to receive sensitive information before sending it to them.
- Ensure that the confidentiality of the sensitive information is protected during transit, for example by encrypting the data.
- Ensure copies of sensitive information are not kept beyond when they are actually required, for example by keeping information "just in case" it might be needed in the future.

All MoJ staff **SHALL** avoid exposing sensitive data to unnecessary risks, in particular by observing all aspects of MoJ [Acceptable Use](#).

Authorisation **SHALL** be sought from the IAO before sensitive information can be moved or shared with a 3rd party. The authorisation itself is captured within the [Data Movement Form](#). the following sub-sections provide guidance on particular types of information sharing common across the MoJ, and to help you complete a DMF.

Internally within the MoJ

Information marked up to and including OFFICIAL-SENSITIVE can be transferred in bulk within an MoJ IT system or domain such as DOM1, without additional controls required to preserve the confidentiality of that information.

Where information is transferred between MoJ IT systems or domains, additional controls might be required to:

- Ensure the information is routed correctly to preserve its confidentiality.
- Maintain the integrity of the data in transit to guard against inadvertent, accidental or deliberate modification.
- Ensure the exchange cannot be repudiated by either party, for example, by enabling proof of sending or proof of receipt.

Information transferred between two MoJ IT systems requires a completed and authorised [Data Movement Form](#) using one of the [data in transit](#) options.

Information sharing with another HMG department

Information shared with another government department **SHALL** be transferred to an assured system. This means the system **SHALL** be assured to the same level as the data being transferred. The transfer **SHALL** take place using one of the [data in transit](#) options. The preference is for information to be transferred using a secure network. However, for low frequency bulk transfers of data, MoJ approved removable media might be more suitable. A completed and authorised [Data Movement Form](#) is required.

Information sharing with external 3rd parties

Any transfer of sensitive data to a 3rd party, including sub-contractors or service providers, **SHALL** be authorised by the relevant IAO. An appropriate contract, [Data Movement Form](#), and Non-disclosure Agreement (NDA) **SHALL** be in place prior to the transfer.

Where the information is OFFICIAL-SENSITIVE, it **SHALL** be transferred to an assured system, assured to the same level as the data being transferred, provided by the external 3rd party, using one of the [data in transit](#) options.

Any transfer to a 3rd party **SHALL** be undertaken with appropriate security controls in place, using the guidance from this document, and seeking advice from the MoJ [Security team](#) as required.

Sharing across an unsecured network

Sensitive data **SHALL** be encrypted prior to being transmitted over an unsecured network such as the Internet. The encrypted data may then be sent via file transfer or as an email attachment.

Ideally, both sender and recipient should check the integrity of data before and after transmission. This includes checking for malicious content, and for evidence of tampering during transit.

Using commercial encryption products for low sensitivity information

Where there is a business requirement to do so, sensitive information may be shared with a 3rd party using a commercial grade encryption product such as SecureZip. Further information on the use of SecureZip can be found in [Using SecureZIP](#).

Note: File encryption does not protect the name of the file. This could reveal clues as to the nature and importance of the encrypted data. Encrypted files should be given innocuous names for transmission. If the data is contained in numerous small files, these should be collected together into a single archive ("zip") file. This archive should then be encrypted. Each file or archive should be sent separately, rather than attaching multiple encrypted files to a single email.

Sharing information higher than OFFICIAL

Where there is a business requirement to share information classified higher than OFFICIAL, advice **SHALL** be sought from the [Security team](#) prior to completing a [Data Movement Form](#).

Data Movement Form (DMF)

The Data Movement Form (DMF) is available [here](#).

The purpose of the DMF is to ensure that the movement of information assets is secure, and in compliance with the [Government Functional Standard - GovS 007: Security](#).

Failure to fulfil or comply with the controls and measures identified within the DMF will lead to unnecessary risk or exposure for the MoJ, or the relevant Information Asset Owner (IAO), or the Senior Information Risk Owner (SIRO).

A DMF **SHALL** be completed, and approval received from the [Security team](#), for the following scenarios:

- Data is being moved or shared by using a physical storage device to transfer the information. An example is where you use a "memory stick", a USB drive, a storage array, or some other removable media. The DMF in this scenario focuses on the data being moved or shared.
- Data is being moved or shared by electronic (network) communication, where the movement is from an MoJ IT system to an external party. An example is using secure file transfer or approved email to transfer the information. The DMF in this scenario focuses on the data being moved or shared.
- An asset (a "data bearing asset") is being moved to, or transported by, an external party. This might be as a result of an office move, or because the asset is being decommissioned. The asset might contain or process MoJ information. Examples of data bearing assets include laptops, servers, multi-functional devices, and any other data bearing peripherals. The DMF in this scenario focuses on the asset being moved or transported, rather than the MoJ information that the asset might contain or process.

A DMF **SHALL** be submitted to the [Security team](#) for information purposes, in the following scenarios:

- Data is being moved or shared by electronic (network) communication, where the movement is entirely within or between MoJ IT systems.
- Data is being moved in full compliance with the already-approved service design and operation specification and procedures.
- An asset (a "data bearing asset") is being moved but remains within the MoJ or its supplier-provided and MoJ-approved facilities at all times.

Note: In the informational scenarios, a DMF is only expected the first time a data movement or sharing takes place. Subsequent, repeat instances of the movement or sharing, do not require a re-submission of the DMF. For example, when setting up a backup process as part of an approved service design, a DMF is created and submitted to the [Security team](#) for information purposes, but does not need to be re-created or re-submitted for each backup occurrence. If the implementation or process for the data movement or sharing changes, for example a new backup technology or process is deployed, then a fresh informational DMF is required.

In any case of doubt, it is always advisable to complete a DMF and await approval or other feedback from the [Security team](#).

Using SecureZIP

SecureZip is a compression and encryption product which can be used to encrypt sensitive data for use in removable media and email based information transfers.

Note: SecureZip can produce "self-extracting" encrypted files that are executable programs which are likely to be blocked by network firewalls or email content checkers.

The general rules for transmitting a password to a recipient are:

- Never transfer the password with the encrypted file, or even over the same communication channel. Use an alternative method, for example if an encrypted file is sent by email, communicate the password or key via SMS text message, letter, fax or phone call.
- Transfer the encrypted data file first. Only send the password or key after the recipient has confirmed receipt of the file.
- Avoid detailing the purpose of a password when it is sent.
- Avoid re-using passwords and demonstrate good security discipline to 3rd parties by creating a completely new password or phrase for each transmission.

More guidance on password best practices is [available](#).

General enquiries, including theft and loss

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

- Tel: 0800 917 5148
- [MoJ Service Portal](#)

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

Government Classification Scheme

The Government Security Classification (GSC) system has three levels: OFFICIAL, SECRET, and TOP SECRET.

The GSC was issued by the Cabinet Office in 2018: <https://www.gov.uk/government/publications/government-security-classifications>

OFFICIAL

This is the majority of information that is created or processed by the public sector.

Includes routine business operations and services, some of which could have damaging consequences if lost, stolen, or published in the media, but which are not subject to a heightened threat profile.

This classification applies to the vast majority of government information including general administration, public safety, criminal justice, and law enforcement, and reflects the fact that reasonable measures need to be taken to look after it and to comply with relevant legislation such as the Data Protection Act, Freedom of Information Act, and Public Records Acts.

OFFICIAL-SENSITIVE

A limited amount of information is particularly sensitive, but still comes within OFFICIAL if it is not subject to the threat sources for which SECRET is designed, even if its loss or compromise could have severely damaging consequences. The need to know principle **SHALL** be rigorously enforced for this information, particularly where it might be shared outside of a routine or well understood business process. There are very few activities where all related information or cases require the OFFICIAL-SENSITIVE marking, though this might apply to assets previously marked as CONFIDENTIAL. Across a range of information assets which were previously normally marked as PROTECT or RESTRICTED, there might be individual cases/instances which are more sensitive (some of which might be marked CONFIDENTIAL on an individual basis). This more sensitive information is identified by adding 'SENSITIVE', and must therefore be marked 'OFFICIAL-SENSITIVE'. This marking alerts users to the enhanced level of risk and that additional controls are required.

SECRET

Very sensitive information that justifies heightened protective measures to defend against determined or highly capability threats.

Where compromise might seriously damage military capabilities, international relations or the investigation of serious organised crime.

Use of SECRET **SHALL** only be used where there is a high impact and a sophisticated or determined threat (elements of serious and organised crime, and some state actors):

- Classified material received from Other Government Departments (OGDs) or agencies relating to national security and counter-terrorism.
- Intelligence and investigations relating to individuals of interests to security agencies.
- Information that might seriously damage security and intelligence operations.
- Information affecting the ability to investigate or prosecute serious or organised crime.
- Personal/case details where there is a specific threat to the life or liberty of an individual such as protected witness scheme records.

The concept of sophisticated or heightened threat doesn't only apply to those with a high technical (IT) attack capability, but might apply to criminals who have a developed capability to intimidate or coerce individuals. If disclosure of information might result in serious physical harm or put a life at risk because there is a real and highly

capable threat present, the information **SHALL** be tightly controlled. **SECRET SHALL NOT** become the default status for material just because of the type of case or potentially severe consequences such as murder trials, or where there is a threat to life. The threat capability **SHALL** also be present.

TOP SECRET

HMG's most sensitive information, requiring the highest levels of protection from the most serious threats.

Where compromise might cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

This classification remains for information of the highest sensitivity relating to national security and subject to highly capable threat sources. There is no change to controls at this level. Any business area holding or expecting to hold information at this level **SHALL** contact the Departmental Security Officer to agree controls.

Applying the classification system

The following considerations apply:

- Staff and delivery partners are responsible for ensuring that all information is looked after with care, to enable the business to function as well as meeting privacy needs.
- The majority of MoJ and wider government information will fall into the **OFFICIAL** tier; there is a significant step up to **SECRET** and **TOP SECRET** which are essential for national security and the very highest threat areas.
- **OFFICIAL** provides for a general and sufficient level of control of information (including for systems holding such information) which is not subject to heightened threat sources. Within this, there is flexibility to apply additional operational controls to reflect sensitivity.
- In most areas of MoJ activity at **OFFICIAL**, staff should continue to follow existing business instructions and procedures for handling information that apply to those activities. Such instructions should include provisions for identifying and dealing with more sensitive cases.
- The 'Working with Official information' desk aid and handling rules should be referred to when receiving, handling or creating information in any format, which is not routine or covered by general processes or instructions.
- Material at **OFFICIAL** does not require a marking to be applied, but must be protected in accordance with the handling rules and any local instructions. However, information assessed to be particularly sensitive must be marked **OFFICIAL-SENSITIVE**, giving a clear warning that strict control of access and special handling apply (see below).
- Staff are expected to comply with local instructions and minimum controls, but need to exercise common sense in situations where applying a control is not possible or would seriously hinder effective business or safety. In all but the most urgent cases, seek approval from your manager or the Information Asset Owner before adopting lesser controls. Decisions must be risk based, and the assessment must be recorded at the earliest convenient opportunity.
- Existing material with former protective markings including **UNCLASSIFIED**, **PROTECT**, and **RESTRICTED** does not need to be retrospectively reclassified. See the [transition note](#) in this guidance.
- Descriptors, such as **PERSONAL** or **COMMERCIAL** are no longer used. In exceptional circumstances or where the recipient might not recognise the sensitivity of the information being sent, authors may include 'handling instructions' in a document or email to draw attention to particular requirements.
- The security officer for your part of the MoJ should be consulted to agree controls if you receive, handle or otherwise process any information at **SECRET** or **TOP SECRET**.

Controls

At **OFFICIAL**, any local instructions or operating procedures should continue to be followed. These should assist staff in identifying any cases that require the **OFFICIAL-SENSITIVE** marking.

This guidance note and the desk aid entitled "Working with Official information" provide some general rules. You might also need to refer to local intranet pages or the handling rules if creating or processing any non-routine material.

Controls should be consistent with the minimum controls set out in the Handling Rules. These must be applied to all information within **OFFICIAL** and are adequate for most information, providing defence against the sort of threats faced by a major company. These threats include, but are not limited to, 'hacktivists', single issue pressure groups,

investigative journalists, competent individual hackers, potentially aggrieved participants or users of the justice system, and the majority of criminal individuals and groups.

Business areas or Information Asset Owners (IAOs) should review risks to their information, and ensure local procedures are in place, adopting additional controls where needed.

The Handling Rules document identifies additional considerations for some aspects of control. Business areas or IAOs might decide to adopt more robust controls in these areas, particularly for material marked OFFICIAL-SENSITIVE or where information is moved, transmitted or otherwise communicated outside of the secure office environment.

Controls should be applied proportionately for information which would previously have been 'unclassified'. Such information still needs looking after if it is required for the job, but might not require controls designed to provide confidentiality.

If IAOs or staff are considering classifying any new assets or reclassifying any existing assets as SECRET or TOP SECRET, they should consult their IA lead and security adviser, or with MoJ security in relation to technical threats, to determine whether a heightened threat might be present, and to agree necessary controls.

Marking of information

Marking is only needed for information which is OFFICIAL-SENSITIVE, SECRET or TOP SECRET. Classifications can be added to information in many different ways but the most important thing is that the marking is clearly visible to anyone using or receiving the information.

This could mean:

- Marking the top and bottom of documents, clearly, in CAPITALS, and CENTRED in the header and footer.
- Showing the marking in the subject line of emails:
 - Type OFFICIAL-SENSITIVE at the start of the subject line, in CAPITALS.
 - Remember to consider whether material that is sensitive needs to be sent, and whether it is safe or appropriate to send if the recipient is outside a secure government network.
 - You must not email anything at SECRET or above.
- Marking the front of folders or binders:
 - Apply clearly in a prominent position in CAPITALS.
 - Apply the highest classification of any of the contents.

Material that needs marking must be transmitted securely. The classification of contents must not be visible on an external envelope sent by post or courier.

Transition to the classification system

For information bearing the 'old' markings, the following guidance should be followed to ensure appropriate handling. Unless there are specific instructions to the contrary, staff are expected to maintain current levels of control and use existing IT systems on which information is currently held or processed.

The old protective markings do not automatically read across, particularly at CONFIDENTIAL.

- All material up to and including RESTRICTED becomes OFFICIAL.
- Much material at CONFIDENTIAL becomes OFFICIAL, but some might become SECRET.
- Only a limited amount of material at RESTRICTED needs marking as OFFICIAL-SENSITIVE.
- CONFIDENTIAL material moving into OFFICIAL is likely to require marking as OFFICIAL-SENSITIVE.

Old marking	New classification	Examples
UNCLASSIFIED or not protectively marked.	Treat as OFFICIAL (unmarked). Where controls prevent otherwise safe sharing of non-sensitive information, IAOs have some discretion to relax controls, provided any relaxations are specific to their assets and have no wider risk consequences, such as for the security of IT assets and government network code of connection.	Public notices and leaflets, published information, information that doesn't contain personal data or other sensitive content, and training materials.
PROTECT.	If information relates to general administration, treat as OFFICIAL (unmarked). Where used for personal data, maintain existing controls. Individual case records containing particularly sensitive content need to be marked OFFICIAL-SENSITIVE, though these instances may already be marked RESTRICTED or CONFIDENTIAL.	Documents containing personal data such as personnel records, citizen or offender case records, and general administration not intended for publication.
RESTRICTED.	<p>If it relates to general administration, there should be a presumption that it can be treated as OFFICIAL (unmarked).</p> <p>You need to consider whether the subject matter is particularly sensitive and there is a need to rigorously enforce access controls, in which case material may additionally require handling or marking as OFFICIAL-SENSITIVE. Anything with this level of sensitivity might already have agreed handling constraints. If in doubt, discuss with the Information Asset Owner.</p>	<p>General administration, policy documents, commercial documents, or case records.</p> <p>Particularly sensitive case records, contentious policy drafts and advice, and sensitive negotiations.</p>
CONFIDENTIAL hard copy previously received from another Department.	Check with the author or originating Department. The presumption should be to treat as OFFICIAL-SENSITIVE and continue with current handling controls, unless there is a clear national security aspect or it relates to protected witnesses, in which case treat as SECRET. If you want to reproduce content in an electronic document, check the classification with the author or originating Department. See the note after the table.	
CONFIDENTIAL electronic copy received by secure government network or held on stand-alone system used for CONFIDENTIAL.	Continue to observe the operating instructions for the system you are using. Continue to use the secure government network for any reply, and use the marking applied by the original author. Otherwise, adopt controls for OFFICIAL-SENSITIVE. See the note after the table.	
SECRET.	Continue to treat as SECRET, subject to any formal review of the classification of the information assets involved in the particular area of activity. If hard copy, treat as SECRET and log, store, move and dispose of accordingly. If held on a stand-alone system currently rated at SECRET, treat as SECRET and observe the operating controls for the system.	Material relating to national security or counter-terrorism, and some protected witnesses.

Note: Electronic records marked CONFIDENTIAL should not be processed or saved on the MoJ existing standard networks such as DOM1 or Quantum, or on electronic document management systems unless or until the originator

or Information Asset Owner has issued revised guidance allowing the information to be handled at OFFICIAL, including OFFICIAL-SENSITIVE, and the system has been rated to hold material at OFFICIAL, with any additional access controls, or the system reclassified as SECRET.

Contact details

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

Information classification, handling and security guide

All Ministry of Justice (MoJ) employees interact with information, and are responsible for its protection. Information security must be considered during the process of designing, maintaining, and securing the MoJ's IT systems that are used to process information.

However, not all information warrants the strictest levels of protection. This is why information classification is so important to the MoJ – to ensure that the department can focus its security efforts on its most sensitive information. Information security must be proportionate to the security classification of the information, and must be considered throughout the information lifecycle to maintain its confidentiality, integrity, and availability.

Classifying information

The three information security classifications the MoJ uses are OFFICIAL, SECRET, and TOP SECRET. This follows the [HMG Government Security Classifications Policy](#).

Each information security classification has a minimum set of security measures associated with it that need to be applied. These security measures might change, depending on the information lifecycle stage.

Classification	Description
OFFICIAL	All information related to routine business, operations, and services. If this information is lost, stolen, or published, it could have damaging consequences, but is not subject to a heightened threat profile. For regular, unsupervised access to OFFICIAL information, someone would be expected to have achieved Baseline Personnel Security Standard (BPSS) assessment.
SECRET	Very sensitive information that requires protection against highly sophisticated, well-resourced, and determined threat actors. For example, where compromise could seriously damage military capabilities, international relations, or the investigation of a serious crime. For regular, unsupervised access to SECRET information, someone would be expected to have passed National Security Vetting Security Check (SC) clearance. In exceptional circumstances, someone with BPSS might be granted occasional supervised access to UK SECRET assets, or be required to work in areas where SECRET or TOP SECRET information might be overheard.
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.

Securing the MoJ's information must be done with a combination of information security measures:

Type of Measure	Description
PERSONNEL	Personnel should be aware of their security responsibilities and in turn acquire security clearances and undertake training to support the MoJ's information security objectives.
PHYSICAL	Tangible measures that prevent unauthorised access to physical areas, systems, or assets.
TECHNICAL	Hardware or software mechanisms that protect information and IT assets.

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	<p>All information related to routine public sector business, operations and services.</p> <p>Almost all personal information falls within the OFFICIAL classification.</p> <p>OFFICIAL-SENSITIVE is not a separate security classification. It should be used to reinforce the "need to know" principle, beyond the baseline for OFFICIAL.</p>	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.
- Information posted on the intranet.
- Supplier contracts.
- Information and data you use to build a database, such as database secrets, record types, and field types.
- Most production data.
- Most non-production data.

OFFICIAL means that the MoJ's typical security measures are regarded as sufficient.

OFFICIAL-SENSITIVE whilst not a formal classification, should be used sparingly, so that its effectiveness is not weakened. This is especially important when you consider that **OFFICIAL** is already well-protected.

Use **OFFICIAL-SENSITIVE** when you want to remind users to be careful when handling information. This asks them to use extra care, beyond what is expected for the baseline **OFFICIAL** classification.

SECRET

The threshold for classifying information as **SECRET** information is very high. It is unlikely that you will encounter **SECRET** information in your day-to-day job.

SECRET information should not usually be handled unless you have sufficient and valid clearance. If you have gained access to information that you believe is **SECRET**, contact the [Security team](#) immediately.

To help decide whether some information should be classified as **SECRET**, ask yourself a simple question:

If a hacker gained unauthorised access to the information, could it compromise the security or prosperity of the country?

The answer is most likely "No". In that case, you should consider using the **OFFICIAL** classification.

TOP SECRET

If the threshold for classifying information as **SECRET** is very high, the threshold for classifying information as **TOP SECRET** is extremely high. It is very unlikely that you will encounter **TOP SECRET** information in your day-to-day job.

TOP SECRET information should not be handled unless you have sufficient and valid clearance. If you have gained access to information that you believe is **TOP SECRET**, contact the [Security team](#) immediately.

To help decide whether some information should be classified as **TOP SECRET**, ask yourself a simple question:

If a hacker gained unauthorised access to the information, would it directly and immediately threaten the national security of the country?

The answer is most likely "No". In that case, you should consider using the **OFFICIAL** or **SECRET** classification, as appropriate.

Reclassifying information

The asset owner has responsibility for reclassifying an asset. If another user has reason to believe that an asset is incorrectly classified or has an incorrect handling caveat, they should normally discuss this with the asset owner. The other user cannot unilaterally reclassify the asset.

The exception is where the asset might need a higher classification than that assigned by the asset owner. The reclassification must still be communicated to the asset owner, for consistency. If it is agreed that the classification should be increased, check with the Security Team (security@justice.gov.uk) whether additional actions are required to protect the material.

Reclassification examples

When deciding whether it is appropriate or desirable to reclassify information, a useful model is to consider what audience might get value from accessing the information. For example, if a hostile country might want the information, then the information might well be best classified as **SECRET**. Alternatively, a reclassification decision might be required as a result of changing threat advice from intelligence agencies.

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.	

Type	Measure	Example
TECHNICAL	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.	
	The MoJ has additional requirements when moving assets which can be found in the HMG Government Security Classifications Policy .	A software developer working from a flatshare should take calls in private, and use headphones and a privacy screen.
	Transferring information from one location to another requires planning and preparation, including a risk assessment. More information on this is available in the HMG Government Security Classifications Policy , and from your manager.	A technical architect working on the requirements for a new MoJ platform should lock their laptop before leaving their desk.
	Protect information "at rest" by using appropriate encryption.	In the development of a new cloud-hosted solution, the following criteria should be considered: remote access connections and sessions are encrypted using an appropriate VPN; information stored "at rest" on end user devices and the cloud is encrypted; information in transit between the end user and the cloud service, such as payment services, is encrypted; and the cloud service used is a Digital Marketplace (GCloud) service.
	Appropriate encryption is also necessary when protecting information in transit.	When using any services over the PSN, make sure you fully read the agreements that you make with the service provider for details and definitions about the data you use or transfer using the service, to ensure you understand the risks to compliance, confidentiality, integrity, and availability.
	Digital Marketplace (GCloud) services can be used for OFFICIAL information.	
	You must not use removable media such as an USB memory stick unless it is unavoidable. When you have to use one, it must be MoJ issued, encrypted so that the effects of losing it are minimised, and the data erased securely after use.	

Note: Different information security measures might be applicable throughout the information lifecycle. It is important continually to evaluate security classifications and their corresponding measures. Refer to the [HMG Government Security Classifications Policy](#) for further guidance.

Handling and securing **SECRET** information

Type	Measure	Example
PERSONNEL	Make sure employees and contractors undergo Security Check (SC).	A contractor working with the MoJ Security Team must have at least SC before being allowed to access SECRET information.
PHYSICAL	Consider using multiple layers of security to protect SECRET information. SECRET information should be held on a secure computer network which is physically isolated from unsecured networks and the internet.	Imagine you are moving locations for a server used to host SECRET information. The encrypted server is secured in a locked and monitored room in 102 Petty France. You have now decided to move it to 10 South Colonnade. This should only be done after relevant parties, including the data owner, line manager, and the system owner, have reviewed and accepted the risks associated with this transfer. The transfer should then be handled by two SC-cleared individuals, for example, employees of a specialised commercial courier company.
	Transferring SECRET information from one location to another requires planning and preparation, including the completion of a Risk Assessment and the use of SC-cleared personnel. More information on this is available in the HMG Government Security Classifications Policy and from your manager.	
TECHNICAL	SECRET information at rest should be protected with very strong encryption. Contact the MoJ Security team for more information.	
	Care should be taken to ensure that SECRET information in transit is only shared with defined recipient users through assured shared infrastructure or using very strong encryption.	
	SECRET information should be processed on IT systems which have been approved for the SECRET threat model. Advice on what commercial IT systems meet this requirement is available from the MoJ Security team .	

Note: Different information security measures might be applicable throughout the information lifecycle. It is important continually to evaluate security classifications and their corresponding measures. Refer to the [HMG Government Security Classifications Policy](#) for further guidance.

Handling and securing TOP SECRET information

Type	Measure	Example
PERSONNEL	Ensure employees and contractors undergo Developed Vetting (DV) security clearance checks.	A contractor working with the MoJ Security Team should have at least DV clearance before being allowed to access TOP SECRET information.
PHYSICAL	<p>Handling and storing TOP SECRET information requires exceptional planning, monitoring, and record-keeping.</p> <p>Working remotely with TOP SECRET is not permitted due to the extreme sensitivity of the information.</p> <p>Transferring TOP SECRET information from one location to another requires even greater planning and preparation than for SECRET information, including the completion of a Risk Assessment by senior management and the use of DV-cleared personnel. More information on this is available in the HMG Government Security Classifications Policy and from your manager.</p>	<p>Imagine you are moving locations for a server used to host TOP SECRET information. The encrypted server is secured in a locked and continuously monitored room in 102 Petty France. You have now decided to move it to 10 South Colonnade. This should only be done after you, your manager, and senior managers have reviewed and accepted the risks associated with this transfer. The transfer should then be handled by two DV-cleared individuals, for example, employees of a specialised commercial courier company. When it happens, local police may need to be informed and involved in providing an additional layer of security.</p>
TECHNICAL	When physical security measures cannot be used, TOP SECRET information at rest should be protected with extremely strong encryption. Contact the MoJ Security team in these circumstances.	

Type	Measure	Example
	<p>Care should be taken to ensure that TOP SECRET information in transit is only shared with defined recipient users through accredited shared infrastructure or using extremely strong encryption.</p> <p>TOP SECRET information should be processed on IT systems which have been approved the TOP SECRET threat model. Advice on what commercial IT systems meet this requirement is available from the MoJ Security team.</p>	

Note: Different information security measures might be applicable throughout the information lifecycle. It is important continually to evaluate security classifications and their corresponding measures. Refer to the [HMG Government Security Classifications Policy](#) for further guidance.

Note: For further information on statutory disclosures and transfer to national archives, please refer to the [HMG Government Security Classifications Policy](#).

Contact details

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

Information Classification and Handling Policy

This document provides the core set of IT security principles and expectations on the handling and classification of information on Ministry of Justice (MoJ) IT systems.

The MoJ stores and processes a wide variety of information, some of which attracts an HMG protective marking or contains personal information. The MoJ has a duty to protect all the information stored and processed on its IT systems.

This policy outlines the Information Classification and Handling Policy for all information held on MoJ IT systems.

Scope

This policy covers all staff (including contractors and agency staff) who use MoJ IT systems.

The overarching policy on information classification and handling is maintained by [MoJ Security](#). This document only contains IT specific policies which are in addition to the overarching policy.

The overarching policy can be found [here](#).

All Users **must be** made aware of the Information Classification and Handling Policy, and provided with security awareness training which covers this policy.

All Users **must be** provided with refresher security awareness training which covers this policy every 12 months.

Inventory of assets

All information assets need be identified and have a nominated asset owner, to help ensure that the appropriate protection of these assets is maintained.

Examples of what an information asset constitutes are:

- Databases and data files.
- System documentation.

- User manuals, training material, operational or support procedures.
- Security documentation such as RMADS or disaster recovery plans.
- Archived backup data.

The list of information assets and associated Information Assets Owners is coordinated and maintained by individual MoJ business groups, where the responsibility resides with the business group SIRO.

All MoJ business groups **must maintain** a list of information assets, their associated named Information Asset Owner (IAO), and which IT systems they reside on.

Note: Some information assets might not be held on IT systems.

Deriving a classification

At the MoJ, all information assets are assessed against HMG guidance on business impact, and HMG guidance on the protection of personal data. This assessment is used to select the appropriate classification from the [Government Security Classification scheme](#).

All information assets stored or processed on MoJ IT systems **must be** assessed for a Business Impact Level, where an impact level for the Confidentiality, Integrity and Availability for each asset is derived.

The Asset Owner is responsible for determining the classification that applies to an asset.

All users are responsible for applying the appropriate classification to information assets created or handled on an IT system, where a pre-existing classification does not exist.

Note: As outlined in the [MoJ IT Security Policy](#), all MoJ data and assets must have IT security controls designed and implemented to protect Confidentiality, Integrity, and Availability.

Further information on the criteria and derivation for classification can be found at: <https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/classifying-information/>.

Reclassifying information

The asset owner has responsibility for reclassifying an asset. If another user has reason to believe that an asset is incorrectly classified or has an incorrect handling caveat, they should normally discuss this with the asset owner. The other user cannot unilaterally reclassify the asset.

The exception is where the asset might need a higher classification than that assigned by the asset owner. The reclassification must still be communicated to the asset owner, for consistency. If it is agreed that the classification should be increased, check with the Security Team (security@justice.gov.uk) whether additional actions are required to protect the material.

Application of Government classification

The Government classification scheme defines how information should be labelled and handled. Output from IT systems containing information that is classified must carry classification labels where it is OFFICIAL or higher. This includes, but is not limited to, printed reports, removable media, electronic messages (such as email) and file transfers.

All IT hardware and removable media assets **must** be labelled with the highest classification from among each of the individual information assets stored or processed on it.

Note: This classification might be reduced if sufficient security controls are applied, for example whole disk encryption, and if there is agreement with the system assurer or Chief Information Security Officer (CISO).

All output from an IT system **must** be given the classification of the highest of each of the individual information assets contained within that output.

Where applying a classification label is not feasible, an alternative method **must be** agreed with the system assurer or CISO.

Further information on the criteria and derivation for classification can be found at: <https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/classifying-information/>.

Information handling on MoJ IT systems

The MoJ policy for handling classified material applies to all MoJ IT assets and all outputs from an IT system.

Contact details

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

Media handling

Removable media

Any Ministry of Justice (MoJ) systems or removable storage media used for work purposes must be encrypted to MoJ security standards. Security encryption is a mandatory government measure, and one of the most important methods we have to protect MoJ information.

Related information

[Security in the office](#) on page 117

What is 'removable' media?

Laptops and [USB memory sticks](#) are the MoJ's most commonly used items of removable media. Removable storage media covers items available to users, such as USB memory sticks, writeable CDs/DVDs, floppy discs, and external hard drives.

Strictly speaking, magnetic tapes are also removable storage media, but it would be very unusual for the average user to have access to or to use magnetic tapes for business purposes.

MoJ security guidance specifies that USB memory sticks and other user-removable media should not be used to store departmental data. Only in exceptional circumstances, and where there is compelling business justification, should MoJ-approved USB sticks with device encryption be used.

USB memory sticks

This guidance is intended to ensure that MoJ data remains secure, and to mitigate the potential impact of lost data sticks.

1. You must only connect approved external removable storage media to MoJ systems.
2. Connecting non-approved memory sticks is a breach of MoJ security guidelines, and could result in disciplinary action.
3. If there is a genuine business requirement to save, retrieve or transfer data via removable media, fill in one of:
 - [Removable media business case form](#)
 - [Data Movement form](#)

Additional guidance information is available about the [Data Movement form](#). When the form is ready, send it to: security@justice.gov.uk.

4. Each request is evaluated by MoJ Operational Security, with a view to recommending the safest and most appropriate method to contain risk of loss.
5. Normally, you'll get a response within 5 working days.
6. Requests to use a memory stick or other removable media will normally only be granted when there is no other practical alternative. Where approval is granted, only encrypted memory sticks or other removable devices provided by the MoJ are allowed. Use of memory sticks or other removable devices will be subject to stringent conditions, and permitted only after user training.

If you need further assistance or information about this process, [ask](#).

How do I know if my laptop, or USB stick, is encrypted?

All equipment provided through the MoJ's recognised central procurement systems are encrypted and protected to MoJ security standards. You must use MoJ processes to obtain any equipment used for business purposes, including mobile computing devices and removable media.

What's expected of you

Keeping MoJ information safe is everyone's responsibility. Anyone using portable computing equipment must take particular care to safeguard the equipment and the information stored on it. Failure to do so may result in disciplinary procedures.

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 through 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

The following organisations are approved to help you with secure disposal of equipment:

- Euro-Recycling: info@euro-recycling.co.uk
- Data Eliminate: info@dataeliminate.com

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.

Destruction method

Covers assets that have reached end of life, and need to be physically destroyed onsite or offsite.

Note: If the data is encrypted, then only the key needs to be deleted or erased, and the table does not need to be followed.

If the table does not cover your exact requirement, contact security: security@justice.gov.uk

Note: When disposing of SECRET or TOP SECRET equipment or materials, always contact security: security@justice.gov.uk

Equipment or asset type	Data deletion method	Destruction method
Flash (USB)	Delete the data, or erase using manufacturer instructions.	Destroy using commercially available disintegration equipment, to produce particles of a maximum of 6 mm in any direction.
Hard disk drive. Note: This includes data centre disk drives.	Overwrite the entire storage space with random or garbage data, verifying that only the data used to perform the overwrite can be read back.	Break the platters into at least four pieces. This can be carried out either manually or by using a commercially available destruction product suitable for use with hard disks. Alternatively, apply a lower level degauss (refer to the explanation after this table), and then apply a destructive procedure that prevents the disk from turning. For example, punch holes into the platters, or twist or bend them.
Magnetic tapes and floppy disks Note: This includes data centre tape drives.	Overwrite the entire storage space with random or garbage data, verifying that only the data used to perform the overwrite can be read back.	Destroy using a commercially available shredder that meets a recognised international destruction standard. Particles of tape should be no larger than 6 x 15 mm. Alternatively, apply a lower level degauss and then cut the tape to no larger than 20 mm in any direction.
Optical media	Data deletion is not possible.	Shred or disintegrate using equipment that meets a recognised international destruction standard. Particles should be no larger than 6 mm in any direction.

Equipment or asset type	Data deletion method	Destruction method
Monitors	Overwrite on-board storage by displaying non-sensitive data on the screen for a few minutes before powering off. Note: If a monitor screen has legible “burn-in” of sensitive information it SHALL NOT be re-sold or donated.	Monitors can be disposed of by: (1) Returning the product to the manufacturer who SHALL align to formal waste disposal responsibilities , or (2) taking the item to a professional waste disposal facility, or (3) reselling or donating to a non-profit organisation, once basic sanitation procedures have been performed. Ensure there is no “burn-in” of sensitive information, and that the device has not reached its end of life. Note: If the end of life monitor contains mercury, it is considered hazardous waste and its disposal SHALL align to WEEE 2013 Regulations using specialist methods such as disassembly to remove the mercury containing backlights for specialist treatment and the separation of the remaining material streams.

Note: A lower level degauss is a process using specialised equipment to erase data totally, by eliminating the unwanted magnetic field (information) stored on tape and disk media.

Owners of the data storage devices are responsible for procuring services that meet the necessary destruction outcomes as described previously.

Wherever possible and appropriate, managers should pool together equipment with that of local colleagues to share service costs.

Data destruction verification

As part of the physical media or data destruction by the MoJ or its suppliers, validation of destruction **SHALL** be carried out. This is to ensure that data handling processes align with the MoJ Asset Management Lifecycle policies. This includes:

1. The MoJ or supplier scans the hard drive or physical media asset tags or barcodes.
2. The MoJ or supplier carries out data destruction (as per the previous table).
3. The MoJ or supplier confirms hard drive or physical media data destruction by providing reasonable proof. This can include:
 - a. Providing an inventory of physical media in their possession.
 - b. Reconciliation carried out on the physical media scanned/received matching the physical media destroyed.
 - c. A witness in attendance to sign a destruction certificate that is be stored in a secure space or network share.

Note: An alternative to the previous steps is to use a leading enterprise erasure tool that provides a certificate aligned to [NIST 800-88 Guidelines for Media Sanitization](#). Such a tool verifies:

1. When the physical media was destroyed.
2. That verification was performed.

If you are based in a London HQ site the Accommodation Team coordinates bulk secure disposal; please contact them in the first instance.

Note: All destruction certificates and destroyed assets **SHALL** be supplied to the MoJ hardware team to update CMDB. This can be done using the technical portal to “Bulk upload CIs - update”, or alternatively by emailing the details to: MoJITAssetManagementTeam@justice.gov.uk.

Transporting data between sites securely

If you have any concerns about moving items between sites securely, contact security: security@justice.gov.uk

Guidance on the transportation of secure data is located in the CPNI guidance: “[10. Transport of sensitive items](#)”.

The previous guidance is also referenced in the CAS Sanitisation Service Requirement, under section “[MIT001 – Keep items secure during transportation](#)” on page 9.

Contact details

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

Working securely with paper documents and files

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

Related information

[Security in the office](#) on page 117

Audience

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

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

POLPPR001: Agencies and arm's length bodies (ALBs) **SHALL** comply with this corporate framework but **CAN** establish their own arrangements tailored to operational needs and **SHOULD** supplement this framework with local policy or guidance for any business-specific risk.

Objective

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

Scope and Definition

This guidance helps you understand the risks involved in working with, sharing, and moving paper documents both inside and outside the office. It covers any information that relates to the business of the MoJ, its stakeholders, or partners, where the information has been printed out or written down on paper.

Note: This guidance applies also to the contents of personal information systems, such as notebooks.

This guidance outlines the basic principles of working securely with paper documents and files.

Context

All MoJ information is valuable. There is a requirement to protect everything that relates to the department's business, including information provided by others.

Note: The protection requirement applies to all information, not just information that is covered by the Data Protection Act or classified under the [government-wide security classification system](#).

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

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

Responsibilities

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

Policy statements

Identifying the correct security level

The MoJ uses the government-wide [security classification system](#) to indicate the level of security that the various types of information require. The different classifications are based upon the harm that would be caused if controls were breached.

POLPPR002: Within the OFFICIAL classification, material does not normally need to have the classification written on it. However, particularly sensitive information **SHOULD** be marked with the OFFICIAL-SENSITIVE handling caveat if it requires more robust access and handling controls to prevent more damaging consequences from disclosure.

POLPPR003: Information handled in the MoJ might not always have a visible classification marking. If any file contains material with a marking, then the cover of the file **SHOULD** be marked with the highest level of any of the contents.

To identify the right security level for information, think about:

- How sensitive that information is.
- Whether it contains personal data that could be used to identify individuals.
- What the consequences might be if the information was compromised or misused.
- Whether the information is likely to be under threat from anyone with a high intercept capability. If so, the information might require marking at a higher classification than OFFICIAL. If you are working with information or documentation higher than the OFFICIAL classification level, contact [MoJ Group Security](#) for specific guidance.

If you are in any doubt, ask your line manager or contact [MoJ Group Security](#).

Allocating security levels and marking

POLPPR004: If you are generating original information, you **SHOULD** apply the [standard rules](#) to decide which classification to use. Do not set security levels higher than necessary. Set the classification that is appropriate at the time. Classification can be altered later if circumstances change, such as when material is no longer embargoed or has been released intentionally for consultation.

POLPPR005: For material at OFFICIAL-SENSITIVE or higher classifications, the classification **SHALL** be written in capitals at the top and bottom of each page of the document. You **SHOULD** use the header and footer facility if creating electronically, and include page numbers by using the format Page x of y. You **SHOULD** only create documents at classification levels higher than OFFICIAL on approved IT systems. If you are working with information or documentation higher than the OFFICIAL classification level, contact [MoJ Group Security](#) for specific guidance. Files and documents **SHOULD** be marked according to the most sensitive piece of information included.

Data Protection Act

If the information in the documents or files can be used to identify living individuals, or could identify living individuals when used in conjunction with other MoJ material, then the information is covered by the Data Protection Act (DPA). The Act covers not only information such as name, address, and date of birth, but also expressions of opinion about or intentions towards an individual.

POLPPR006: Paper-based information that is covered by the DPA **SHOULD** be managed according to the general principles of working securely with paper documents and files set out here.

Handling paper-based information in the office

Think carefully before leaving papers unattended on desks, in the same way that you would avoid leaving your own personal correspondence – or even a purse or wallet – in plain view.

The MoJ has a [clear desk policy](#) that is intended to ensure information is seen only by people who 'need to know' it.

This means:

- Not leaving documents or files on a desk when not being used.
- Locking documents or files in a secure cabinet when you leave the office.

Failure to follow this policy could expose files and papers to the risk of being seen during the working day by other staff, or visitors to the office and, out of hours, by guards and cleaners. Even apparently non-sensitive information should be looked after. Putting papers away also protects them from damage from fire, smoke, or water.

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.

POLPPR007: 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.

POLPPR008: 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.

POLPPR009: 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.

POLPPR010: 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.

POLPPR011: 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.

POLPPR012: 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.

POLPPR012: 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.

POLPPR013: 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.

POLPPR014: 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.

POLPPR015: You **SHOULD** read and follow the [secure waste disposal](#) guidance on the MoJ Intranet before disposing of any document or files.

POLPPR016: 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.

Long-term storage

The MoJ has arrangements for the secure long-term storage of paper documents and files. If you want to keep paper-based information, but no longer need to regular access to it, refer to the information on the MoJ Intranet regarding [keeping, deleting, and disclosing information](#). The [Records and Retention team](#) can provide additional guidance.

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

POLPPR017: If you suspect that the security of the information you work with has been compromised in any way, you **SHALL** [report it immediately](#).

Note: A security breach does not 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 may be no evidence that any information has been lost or interfered with, but there is a clear potential for loss or damage.

Compliance

POLPPR018: 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 a baseline of physical security measures are in place at each site, and receive annual assurance that measures are in place to provide appropriate protection to all occupants and assets, and that these measures can be strengthened when required, such as in response to a security incident or change in the Government Response Level.

POLPPR019: 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, Physical Security advice taken from the Centre for the Protection of National Infrastructure (CPNI), and [Government Functional Standard - GovS 007: Security](#).

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

Physical security advice

Physical security advice can be obtained by contacting [MoJ Group Security](#).

Contact details

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

Access control

User responsibilities

Protecting social media accounts

Hostile attacks on Social Media accounts pose a serious threat to the Ministry of Justice (MoJ) and its reputation. When attacks happen, they quickly become headline news, and can happen to any account, anywhere in the world.

Two types of attacks are common:

- Attempts to render the account useless by 'bombarding' it with messages.
- Attempts to 'take over' the account.

Steps we can all take to protect ourselves

Ensure our passwords are secure

Passwords are the main protection on our accounts, hence ensuring they are secure is vital. The NCSC has produced [guidance](#) on making secure passwords - the summary of which is that picking three random words to make a password (for example RainingWalrusTeacup) is a good policy for securing Social Media accounts.

Check your email details are up-to-date

Most of the time, the first indication you'll have that something is wrong is when an email is sent to you. This could be to let you know that someone is attempting to log into your account, or that someone is trying to reset your password, or more worryingly, that a new device has logged into your account. Hence it is important that you ensure that your email details are up-to-date, and that your email is secure.

Enable Two Factor Authentication

Two Factor Authentication (2FA) involves requiring a random code to be entered before being logged in. These codes are either sent to the user via SMS or email, or generated every 30 seconds by an app or device the user has which relies on a seed key provided by the service. That seed can then be shared amongst a team, allowing for multiple owners or contributors.

If at all possible, SMS generation should be avoided, as it is theoretically possible for phone numbers to be taken over through various attacks, as well as meaning that only one person can receive the code, which isn't ideal if a team is working on a single account.

If you're using email, then it can be sent to a group account, which also allows for multiple owners or contributors - but it's important to ensure that the email is also protected by 2FA.

If you have a spare 10 minutes, watch [this video](#) for an excellent explanation of how 2FA works and why it's important to have it enabled.

Click the links for details on how to activate 2FA for [Facebook](#), [Twitter](#) and [Instagram](#).

Only use trusted third-party applications

In addition to the official applications, there are many tools and third-party applications that might be used to work with social media accounts.

Some of these tools provide useful extra facilities, such as 'scheduled' posts, or helping you post one message to several different social media channels.

The problem is that you have to give your account details to these tools so that they can post to your account.

This is potentially very dangerous:

- An application might post messages on your behalf, that you do not agree with or are unacceptable.
- An application might store or share your account details.

Only use applications that are trusted and approved for use with your social media accounts. For help with this, [contact Cyber Security](#).

Remove 'unused' applications

People tend not to be very good at removing old or rarely used applications. Older applications should be checked regularly to find out if there are any updates.

A good habit is to check your applications once a month or so, and consider:

- Do you still use the application? If not, remove it.
- Whether there is an update available for the application? If so, install it.

As well as increasing safety, removing unused applications frees up storage space on your system.

Check your privacy settings

The whole point of a social media account is to share information. But that doesn't mean you want to share *everything*.

When you first create a social media account, you are normally asked to decide on the privacy settings. These control how much information you share, and who you share it with.

Typical settings that affect privacy include:

- General information about you.
- Your Profile information and photo.
- When you were last active.
- Any status updates.
- Whether you have read direct messages ("Read Receipts").
- Whether others can add you to their groups, possibly without your knowledge or agreement.

But it's very easy to forget to check the settings, from time-to-time, to make sure they are still correct.

A good habit is to check your account privacy settings once a month or so. Information on privacy settings is available for the main social media environments:

- [Facebook](#)
- [Instagram](#)
- [Twitter](#)
- [WhatsApp](#)

For example, in WhatsApp, to prevent someone adding you a group without your knowledge, change your settings: **Settings > Account > Privacy > Groups > My Contacts**. This change means that only people you know (your contacts) can add you to a group.

Limit access to your accounts

You might be tempted to share access to your social media account, for example if you want to have postings regularly, even while you are away.

Avoid sharing access to your social media account. It's easy to forget who the details are shared with. It's also possible that postings might be made on your behalf that you don't agree with, or are not acceptable.

Any MoJ social media accounts that do need to be shared will have proper access controls in place. You should never need to share your account details for work purposes.

If you need more help on this, contact your Line Manager or [Cyber Security](#).

Don't click on suspicious links

Unfortunately, social media postings are a common way of sending you links to malware or other problem material. Postings might also be used to send you 'phishing' attacks.

In the same way that you should be careful with any links or attachments sent to you using email, you should also be suspicious of links or attachments sent to you through social media. This applies to both general postings and messages sent directly to you ('Direct Messages').

For more information, read [this article](#) on the MoJ Intranet.

What to do if your account is bombarded Remember that these attacks are short lived

Due to the amount of organisation and effort required to coordinate such an attack, they do not last long, and like an intense inferno, will soon burn themselves out.

Do not respond to the attack

These attacks are designed to attack the person controlling the account as well as the agency itself. By only responding to messages not involved in the attack - especially those trying to share positive messages, the attackers

will run out of interest far sooner than if you engage them. If they are posting harmful or threatening messages, report the accounts.

In a single sentence - "don't feed the trolls".

Feel free to walk away

Dealing with these attacks can be emotionally draining; even just reading the messages can have a far greater impact on you than you realise. Take breaks in the event of an attack, even if it's hard to - consider going for a walk to force yourself away.

Cyber Security Advice

Cyber Consultants and Risk Advisors

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

System and application access control

Password Managers

[Ministry of Justice \(MoJ\) guidance](#) makes clear that you should have different passwords for different services. These passwords must be complex.

But how do you remember all these different passwords?

The simplest way is to use a [Password Manager](#). If you have lots of different, and complex, passwords for all your accounts, using a password manager makes life much easier.

This article provides guidance on using password managers within the MoJ.

Password managers and vaults

A password manager stores sensitive information in an encrypted form. Password managers are sometimes called password vaults.

In the MoJ, password managers are tools that you might use for your personal accounts. Password vaults are tools that a team of people might use to look after details for shared accounts.

Password vaults usually have extra strong access controls, such as hardware tokens.

Here, we use password manager and 'password vault interchangeably, except when stated otherwise.

When to use a password manager or a password vault

The following table shows when you might use a password manager or vault:

Scenario	Tool	Notes
Single user, personal accounts	Password manager	For accounts that only you use, or have access to, then you would probably store the details in a password manager. An example would be storing the username and password for your work email account; only you should have access.
Multiple users, shared accounts	Password manager or password vault	Some accounts might be shared between a group of users. For example, a team might need to know the password for an encrypted document. If the access required is for a sensitive or operational system, then a more heavily protected tool such as a password vault might be appropriate.

Scenario	Tool	Notes
System access, no human use	Password vault	Some MoJ systems need to 'talk' directly to other systems. No humans are involved in the conversation. The passwords protecting these communications can - and should - be extremely complex. A strongly secured password vault would be ideal for this purpose.

Best practices

The NCSC is [very clear](#):

- "Should I use a password manager? Yes. Password managers are a good thing."

This is helpful for us in the MoJ, as much of our IT Policy and guidance derives from NCSC best practices.

Good password managers

A password manager should never store passwords in an unencrypted form. This means that keeping a list of passwords in a simple text file using Notepad would be A Bad Thing.

Good password managers encrypt the passwords in a file using strong encryption. It shouldn't matter where you store the encrypted file. Storing the list "in the cloud" lets your password manager access the data from any device. This is useful if you are logging in from a laptop, or a mobile device. Storing the passwords locally means the password manager works even when offline.

A good password manager will have:

- Strong encryption for the list of passwords.
- Network access for encrypted lists stored in the cloud.
- A dedicated app but also a pure web browser method for working with your password list.
- A tool to generate passwords of varying complexity.
- The ability to fill in login pages.

What password manager to use

In the [NCSC article](#), they are very careful not to identify or recommend a password manager. This ... caution ... is the reason why we don't say much about password managers within the MoJ guidance.

There are several password managers used within the MoJ. [LastPass](#), [KeePass](#), and [1Password](#) are probably the most popular for personal or team passwords. To determine whether a particular password manager is suitable for work usage, check the [General app guidance](#).

Example password vaults would be Hashicorp Vault, Kubernetes Secrets or AWS Key Management.

For individual use, have a look at LastPass and 1Password. Consider which one you like best, and try it out. When you decide on a password manager, request approval from your line manager to install and use it: "I'm planning to install and use XYZ to manage my passwords, is that OK?".

Refer also to the [Using LastPass Enterprise](#) guidance.

Contact details

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

Passwords

This article provides guidance on passwords and Personal Identification Numbers (PINs) within the Ministry of Justice (MoJ). It helps you protect MoJ IT systems by telling you about choosing and using passwords and PINs. Whenever you encounter the word "system" here, it applies to:

- Hardware, such as laptops, PCs, servers, mobile devices, and any IT equipment.
- Software, such as the Operating System, or applications installed on hardware, or mobile device applications (apps).

- Services, such as remote databases or cloud-based tools like [Slack](#).

This guidance is for all users.

Note: Except where stated, the guidance in this article applies to both passwords and PINs.

Related information

[Security in the office](#) on page 117

General best practices

Note: This section applies to passwords and PINs.

You **SHALL NOT** share your password or account details with anyone, unless you have documented approval to share from your Line Manager or higher senior manager.

If a system or another person provides you with a password, change it before doing any MoJ work on that system. Examples of 'single-use' passwords include:

- Your own account on a work-provided laptop.
- A shared account for accessing a data analytics service.
- All supplier or vendor supplied accounts.

You **SHALL** change a password whenever:

- There has been a security incident involving your account or password. For example, someone guessed your password, or you used it on another account.
- There was a security incident with the service that you access using the password. For example, if someone broke into the system that provides the service you use.
- Your line manager or other authorised person tells you to do so.

When required to change a password, you **SHALL** do so as soon as possible. If you don't change the password soon enough, you might be locked out of your account automatically. The following table shows the maximum time allowed:

Type of system	Maximum time to change a password
Single-user systems, such as laptops	1 week
All other systems	1 day

Best password practices for everyone

Note: This section applies to passwords only, not PINs.

The MoJ password guidance follows [NCSC guidance](#). The NCSC recommends a [simpler](#) approach to passwords. Some agencies or bodies might have specific requirements or variations. Check your team Intranet or ask your Line Manager for more information.

Follow the [CyberAware advice](#) to generate your passwords. Always use a separate and unique password for each account or service.

The most important points to remember are that passwords should be:

- At least 8 characters long.
- No more than 128 characters long.
- Not obvious.
- Not a dictionary word. A combination of dictionary words might be suitable, such as "CorrectHorseBatteryStaple".
- Unique for each account or service.

Best PIN practices for everyone

Note: This section applies to PINs only, not passwords.

Some devices, especially mobile devices, only support numerical passwords, or Personal Identification Numbers (PINs).

If the device supports passwords, then passwords **SHOULD** be used rather than PINs.

If the device supports only PINs, you **SHOULD**:

- Always use a separate and unique PIN for each account or service.
- Ensure the PIN is at least 4 characters long.
- Avoid using obvious PINs, such as 1234.
- Avoid using repeating digits in the PIN, for example 0000 or 9999.

App-based password protection for files

Some applications - including Microsoft Office tools such as Word, Excel, and Powerpoint - provide mechanisms for protecting files. A password controls whether someone can open, or edit, a file.

While these app-based password protection mechanisms are better than nothing, there are three good reasons for avoiding them if possible.

1. You depend on the application to provide and maintain strong password protection. If the password implementation fails, or has a weakness, you might not know about it. This means that you might think your information is protected, when in fact it is at risk.
2. It is tempting to use a standard password for protecting a file within the app, so that other people can share and work with the file. Changing the password becomes "inconvenient". The result is that many versions of the data file are all protected with the same password. Also, if anyone has ever been given the password to access the file, they will always be able to access the file.
3. If you forget the app-based password, there might not be a recovery process available to you.

For these reasons, MoJ advice is that you **SHOULD NOT** use password tools within an app to protect data files that are processed by the app. For example, you **SHOULD NOT** use the password tools with Microsoft Word, Excel, or Powerpoint, to protect MoJ information within files. Instead, either:

1. Store the data files in a shared but secure area, such as the MoJ SharePoint storage facility.
2. Use separate encryption tools to protect data files, separate from the app that works with the data files.

Of these two options, storing data files in a shared but secure area is strongly preferred. The reason is that you can add, modify, or revoke access permissions to the storage area easily.

If you have no choice, and have to use app-based password protection, ensure that the same password is not used indefinitely for a data file. You **SHOULD** use a different password for:

- Each major version of a data file, for example version 2.x is different to version 3.x.
- Any data file where the password is more than three months old.

Note: This advice is a specific exception to the [general guidance](#), that you do not normally need to change passwords.

Password expiry

You don't have to change a password because it is old. The reason is that time-expiry of passwords is an [...outdated and ineffective practice](#).

Some current or legacy systems don't allow passwords that follow MoJ guidance. For example, some mobile devices, laptop hard drive encryption tools, or older computers might not be able to support a mix of character types. For such systems, choose passwords that are as close as possible to MoJ guidance.

Password managers

Use a password manager to help you keep track of your passwords.

These are tools that help you create, use, and manage your passwords. A useful overview is available [here](#).

As passwords become more complex, and you need to look after more of them, it becomes increasingly necessary to use a password manager. For example, development teams in MoJ Digital & Technology use [LastPass](#).

You still need to remember one password. This is the password that gets you into the manager application. Once you have access, the application works like a simple database, storing all the passwords associated with your various accounts and services. Some managers have extra features, such as password generators. Some managers can even automatically fill-in username and password fields for you when during log in.

The password manager database is often stored in the cloud so that you can use it anywhere. The database is encrypted, so only you can open it. That's why your single password key is so important. Without it, you can never get access to the password database again.

Using a password manager for your MoJ account and service details is recommended.

You can find additional useful information about password manager tools [here](#).

Default passwords

Change all default passwords when a new, modified, or replacement system arrives. Complete the changes before making the system available for any MoJ work.

When preparing devices or services for first use, system developers or system administrators **SHALL** configure the default password on the device or service so that it can be used once only. The “first use” of a password forces the user to change the password before the device or service can be used.

Password access attempts

If a password is ever entered incorrectly, a count starts. After at most 10 (ten) consecutive failed attempts at using the correct password, access to the account or system is locked. A successful use of the password resets the count to zero again.

Password reset

If a password lock occurs, a reset is necessary. This requires action by the system administrator or the MoJ IT Service Desk. The process should be like issuing the password for the first time. Other account details are not changed during the reset. This helps avoid losing any work. Checks ensure that an attacker cannot use the password reset process.

Blocking bad passwords

You should not try and use [obvious passwords](#). Attempts to do so will be blocked.

Single-use passwords

Some passwords are 'one time' or single-use. Administrators and developers use these to grant access to a service for the first time. After using the password once, the user **SHALL** immediately change the password.

Single-use passwords are time limited. If they are not used within a specific time after generation, they **SHALL** become invalid.

The following table shows the valid lifetime of a single-use password:

Type of system	Lifetime of a single-use password
Single-user systems, such as laptops	1 week
All other systems	1 day

Contact details

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

Using LastPass Enterprise

What is LastPass?

LastPass is an online password management tool that we make available to you to help you create, store and share passwords. Using it means you no longer need to remember dozens of passwords, just a single primary password. It keeps all your website logins protected, helps with creating new 'strong' passwords and password sharing when required.

LastPass is available as a browser extension for popular browsers and as well as a full software suite (for use outside of browsers) for Microsoft Windows and Apple macOS.

LastPass will securely save your credentials in your own LastPass 'Vault' and then offer to autofill those credentials the next time you need them.

The Ministry of Justice (MoJ) has the Enterprise tier of LastPass.

Who should use it?

MoJ LastPass accounts can be requested by anyone in MoJ Digital and Technology.

At the moment, rollout is limited to technical service or operations teams that have a need for shared passwords.

How to get it

Email lastpass-admins@digital.justice.gov.uk to request access.

Make sure you include in the email:

- which team you're in
- your role in your team
- why you need access

What it can be used for

LastPass can be used for sharing passwords within a team, when individual named accounts cannot be created in the service. A good example is running a shared Twitter account.

Note: If you have a business need for a shared Twitter account, consider using a more enterprise-orientated tool for social media posting, such as [TweetDeck](#) or [Hootsuite](#). You need [formal approval](#) to use tools like these.

Personal use

You **SHOULD NOT** use your MoJ LastPass account to store personal non-work information as it is a work account belonging to the MoJ. You may lose access if you change role. You will lose access entirely if you leave the MoJ.

MoJ LastPass administrators cannot routinely access the contents of LastPass Vaults but can reset accounts to gain access if there is a good reason to do so.

What it shouldn't be used for

LastPass **SHOULD NOT** be used for storing personal passwords, or for storing MoJ documents. Use existing approved MoJ services such as Office 365 or Google Workspace for storing MoJ documents.

You shouldn't use LastPass for 'secrets' that belong to systems, only credentials to be used by humans.

How to use it

Getting started

You will be sent an email to your MoJ work email account inviting you to create your LastPass account. LastPass have ['getting started' guides](#) on their website.

Creating your primary password

You need to create a primary password - this is the only password you'll need to remember.

It must be at least 12 characters long (the longer the better).

You can choose to make it pronounceable and memorable (passphrase) such as `CyberSecurityRules!` or `Sup3rD00p3rc0Mp3X!`, as long as you're comfortable remembering it and won't need to write it down.

There are password guidance standards [here](#).

Your primary password **must** be unique and you should **never** use it anywhere else (including a similar version, for example, by simply adding numbers to the end)

Multi-Factor Authentication

You **must** setup multi-factor authentication (MFA, sometimes known as 2FA) for your MoJ LastPass account.

LastPass has a [guide on setting up MFA](#).

If you don't have an MoJ-issued work smartphone you may use a personal device for MFA.

Sharing passwords

To share a password [create a "shared folder" in the LastPass 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 shared folders when access to the credential(s) is no longer required.

You must not share your LastPass main password with anyone, even your line manager or MoJ security.

Using it overseas

Taking a device (such as personal smartphone) that has MoJ LastPass 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 LastPass applications or uninstall/delete them before travelling outside of the UK and reinstalling when you get back.

Keeping LastPass update to date

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

Need help?

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

If you need help using LastPass such as getting access to shared folders or resetting your primary password as you have forgotten it, contact lastpass-admins@digital.justice.gov.uk

Physical and environmental security

Secure areas

CCTV policy

The policy complements the Ministry of Justice (MoJ)'s overall security policy.

The CCTV Policy 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 the corporate framework, but **MAY** establish their own arrangements tailored to operational needs and **SHOULD** supplement the framework with local policy or guidance for any business-specific risk.

Objective

The MoJ has in place several CCTV surveillance systems installed within its core buildings. This policy details the purpose, usage, and management of the CCTV systems, and the procedures to be followed to ensure the MoJ complies with relevant legislation and the current Information Commissioner's Office (ICO) Code of Practice.

The MoJ has due regard to the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), the Freedom of Information Act 2000, the Protection of Freedoms Act 2012, and the Human Rights Act 1998. The MoJ also has due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012, and the 12 guiding principles contained therein.

This policy is based upon guidance issued by the ICO.

This policy and the procedures it details apply to the MoJ CCTV systems, including security guards' body worn cameras. CCTV images are monitored and recorded in strict accordance with this policy.

The policy is applicable to all buildings owned or occupied by the MoJ, where MoJ monitored CCTV is installed.

The policy is available for download [here](#).

Contact details

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

Entry and exit search policy

The Ministry of Justice (MoJ) "Entry and Exit Search Policy" 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 this framework with local policy or guidance for any business-specific risk.

The policy defines the access controls that are in place when entering and exiting MoJ buildings.

The policy is available for download [here](#).

Physical security advice

Physical security advice can be obtained by contacting MoJ Group Security: mojgroupsecurity@justice.gov.uk.

Contact details

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

Personal mail and parcel delivery policy and procedure

This personal mail and parcel delivery policy applies to all Ministry of Justice (MoJ) 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 Arms 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.

Objective

Following a review by Government Security Centre People and Physical (GSCPP), it is recommended that the MoJ implements a policy on personal and business deliveries, including prohibiting personal parcel deliveries, to

MoJ buildings. This policy prohibits deliveries of personal items to MoJ buildings, to comply with HMG minimum physical standard No.10 on mail or delivery management. For further information regarding this standard, contact mojgroupsecurity@justice.gov.uk.

This provides MoJ employees, contractors, partners and other interested parties with a clear policy on mail deliveries, to prevent attack, damage, or interference (malicious or otherwise) to MoJ assets, and - most importantly - physical harm to MoJ people and the public.

Scope and Definition

For the purpose of this policy, personal deliveries are goods purchased over the internet from online retailers or mail subscriptions that are delivered to an office without a legitimate business need. This policy permits vital work-related courier deliveries to reception, as outlined in the policy statement in this document. Vital work-related deliveries are those required to support a business's function, or to support a business need. Ordering gifts to be delivered for colleagues who are leaving the organisation, or for a special occasion, are not considered to be a business-related activity.

Context

The growth in online shopping has seen an increase in the number of personal parcels delivered to the office, as a convenient location because of onsite staff on hand to receive deliveries that would otherwise be returned to depot. However, receiving personal parcels in reception diverts reception and security staff from their core duties, and presents a significant vulnerability to the building's security: the parcel contents are unknown by reception staff. Reception areas are generally within the main fabric of a building and with no separate ventilation or enhanced blast resistant walls, any hazardous substance or explosive device would have a serious impact throughout the building. The MoJ employs off-site mail screening to mitigate against the chances of hostile mail being accepted into MoJ premises.

Couriers often require a receiver to sign a Proof of Delivery document, stating that the parcel arrived in good condition, which risks the MoJ being liable for accepting the package if contents turn out later to be damaged.

Online retailers recognise the needs of their customers of convenience by offering either "Click and Collect" options, or offering parcel collection facilities in convenient locations. This alternative to office-based deliveries is both convenient and reduces the need for staff to carry parcels on their commute home.

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 MoJ assets.

Policy Statements

Items required for a legitimate business need **CAN** be delivered to the office, provided reception have been notified by email from a verifiable email account (for example a Civil Service or Government contractor) 48 hours before the parcel is to be delivered, or as soon as practicable in the case of next-day or same-day deliveries. The email notification **SHOULD** provide all of the following information:

- Estimated date of delivery.
- Name of Courier.
- Contact details of the recipient(s), who can sign for the parcel and collect it from reception.

MoJ reception produces a list of scheduled deliveries. Before accepting parcels from the courier, reception confirms who the parcel is for, and that it is a pre-approved delivery. Failure to follow this procedure **MAY** result in the need to have the parcel scanned, or it being treated as suspicious and the suspicious package process being adopted; disciplinary action **MAY** be taken.

Compliance

The level of risk and potential impact to MoJ information, assets, and people determines the controls to be applied, and the degree of assurance required. The MoJ **SHALL** ensure 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 must be able to provide evidence that the selection has been made in accordance with the appropriate information security standards ISO27001/27002, physical security advice taken from the Centre for the Protection of National Infrastructure (CPNI), and [Government Functional Standard - GovS 007: Security](#).

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, including specific advice on this guidance, can be obtained by contacting MoJ Group Security: mojgroupsecurity@justice.gov.uk.

Contact details

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

Physical Security Policy

Related information

[Security in the office](#) on page 117

Audience

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

Physical security is the practice of protecting elements of government infrastructure, estates and personnel against attacks or compromises in the physical (tangible, real-world) environment.

This Physical Security Policy 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.

Executive Agencies and Arm's Length Bodies (ALBs) are expected to comply with this corporate framework, but might establish their own arrangements tailored to operational needs, and should therefore supplement this policy with local policy or guidance for any business-specific risk.

Objective

This content provides employees, contractors, partners and other interested parties with a clear policy direction. It requires them to ensure that all necessary physical protective security measures are in place to prevent attack, unauthorised access, damage, or interference (malicious or otherwise) to MoJ assets, and most importantly to prevent physical harm to our people and the public.

Scope and Definition

Physical Security refers to measures that are designed to protect physical locations and the assets, information, and personnel contained within.

This policy sets out the approach to be adopted to manage, develop, improve and assure Physical Security across the MoJ.

It is essential that MoJ business is conducted in an environment where potential threats - including those from both natural and human-made hazards, terrorism, crime, and insider threats - to MoJ assets, information, and personnel have been identified, risk assessed and appropriately mitigated to prevent interference, loss, or compromise (malicious or otherwise). This includes ensuring physical perimeters are protected, and entry controls are in place to provide proportionate protection against natural disasters and terrorist attacks.

Context

This policy sets out a framework to follow a "layered" approach to physical security. It provides suitably secure environments from which the MoJ can operate, to achieve its strategic aims and objectives by implementing security measures in layers, to appropriately protect personnel and assets, including material of differing levels of sensitivity.

This policy provides a high-level organisational objective for the MoJ with regards to Physical Security, supported by **MANDATORY** Physical Security Standards which **SHALL** be followed to ensure compliance, as they represent the minimum measures required to protect the security of assets, information and people.

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.

The most senior grade based at each site, or in "Moderate Risk" and larger sites the Senior Responsible Officer (SRO), has responsibility for ensuring physical security risk assessments are conducted annually. They **SHALL** ensure the action plans created to address identified risks and instigate business continuity activities are up-to-date, clearly communicated, regularly rehearsed, implemented effectively, and readily available, in accordance with their significance, importance, or classification.

Managing the physical security controls of sites occupied by MoJ employees is the responsibility of a contracted provider. The physical security controls include, for example:

- Perimeter control.
- Guarding.
- Site access.

The controls are measured in the form of Physical Security Reviews, as undertaken by the Group Security and Governance Team.

It is the responsibility of those procuring supplier contracts for such physical security measures to ensure that the most up-to-date technical and industry standards are met, and that the technology and processes in place are regularly reviewed to ensure that the security controls remain effective and fit for purpose. This includes technical and industry standards for Closed Circuit Television, Access Controls, Intruder Detection Systems, and any other relevant alarm systems which are managed by a contracted supplier.

Policy statements

Physical Security controls **SHALL** be implemented that are proportionate to the risk appetite of the MoJ, and in adherence with the Information Security Policy and Acceptable Use Policy and other appropriate personnel and information security standards, including successful completion of the [Baseline Personnel Security Standard](#).

All employees must ensure they remain observant, report any suspicious behaviour, and highlight non-compliance. This vigilance will help deter, delay, prevent, or detect unauthorised access to, or attack on, a location, and mitigate the impact should they occur.

Each MoJ occupied premises presents unique physical security challenges. The measures introduced to protect each site **SHALL** take into account the risk categorisation and the physical composition of that site. Effective approaches to Physical Security **SHALL** follow the **MANDATORY** Physical Security Standards.

The most senior grade manager, or SRO in "Moderate Risk" and larger locations, **SHALL** ensure that their site adheres to the Response Level Security Measures Policy, and ensure physical security risk assessment activity is conducted annually, and that the action plans created to address identified risks are implemented.

Compliance

The level of risk and potential impact to MoJ information, assets and people determines the controls to be applied, and the degree of assurance required. The MoJ **SHALL** ensure 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 change in the Government Response Level.

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

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, as warranted.

Physical security advice

Physical security advice, including specific advice on this guidance, can be obtained by contacting MoJ Group Security: mojgroupsecurity@justice.gov.uk.

Public protest and demonstrations policy

This policy provides Ministry of Justice (MoJ) employees, contractors, partners, and other interested parties with enough guidance to take proportionate measures in case of public protest or demonstration.

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

Audience

This policy complements the MoJ overall security policy.

This Public Protest Policy applies to all employees, contractors, partners and service providers, including those on co-located sites and sites owned by other public bodies. This includes employees of other organisations who are based in, or work at, MoJ occupied premises.

POL . PPD . 001: Agencies and arm's length bodies (ALBs) **SHALL** comply with this corporate framework but **CAN** establish their own arrangements tailored to operational needs and **SHOULD** supplement the framework with local policy or guidance for any business-specific risk.

Scope and Definition

Protests take different forms, ranging from action by one person acting alone to a demonstration attended by thousands of people. In some instances, the MoJ might have advance notice of a public protest, in other instances the protests might be unannounced or spontaneous. This policy aims to ensure that the response to all protests are managed proportionately and consistently.

Context

Freedom of speech and the right to peacefully protest is protected by law, both under common law and the Human Rights Act 1998. However, freedom of speech and the right to peacefully protest are not absolute, and the exercise of those rights can be restricted provided any restrictions:

- Are prescribed in law.
- Are necessary and proportionate.
- Pursue one or more of these aims:
 - The interests of national security or public safety.
 - The prevention of disorder or crime.
 - The protection of health or morals.
 - The protection of other's rights and freedoms.

The rights of those protesting need to be balanced with the rights of others to go about their business without fear of intimidation or having serious disruption to their community.

The MoJ **MIGHT** be the subject of protests and demonstration by various activist groups seeking publicity for a specific cause or case.

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.

POL.PPD.002: The building's security team **SHOULD** adapt their process and procedures in line with the advice given to organisations and businesses in central London by the Metropolitan Police Service or their local police force.

Buildings located in Central London, within the Government Security Zone (GSZ), receive information from the GSZ control room about proposed protests – either from information provided by the organisers or through monitoring social media.

Following any public protest or demonstration, the most senior grade based at the site, or in Moderate Risk and larger sites, the Senior Responsible Officer (SRO), has responsibility for ensuring that detailed records are kept of any incidents, including:

- The identity of those involved.
- The date, time and location.
- The behaviour involved.
- The impact, such as damage, injury, or disruption.
- Any warnings issued or other steps taken to defuse the situation.

Policy Statements

POL.PPD.003: The buildings' incident control plan **SHOULD** be reviewed regularly to ensure that it is up-to-date with good communication systems for the Incident Control Officer or Deputy Incident Control Officer to direct matters.

Managing the site, including security detail

POL.PPD.004: The following aspects of site management **SHOULD** be addressed:

- Minimise the number of entry points to the building.
- Ensure the outside areas are clear of debris, dustbins, ladders, tools, or equipment.
- Check that emergency equipment, grab bags, first aid supplies, and personal radios are in place, easily accessible and working properly. It is advisable to test them beforehand.
- Check and test building security and emergency systems.
- Ensure [CCTV coverage](#) is fully operational and can provide the highest recording resolution possible.
- If your building has scaffolding erected or is near scaffolding, let your security staff know.
- Report any suspicious activity to police by dialling 999 in an emergency, or call 101 if not an emergency.

People management and communication

POL.PPD.005: In the days leading up to a planned event, all employees **SHOULD** be fully briefed.

POL.PPD.006: The building **SHOULD** have a strong, visible management presence who **SHOULD** identify themselves to the police in the event of any trespassing or damage.

POL.PPD.007: Security officers, where possible, **SHOULD** be highly visible.

POL.PPD.008: All staff **SHOULD** remain vigilant and report any suspicious activity to security or the police.

POL.PPD.009: All members of staff **SHOULD** be fully aware of any emergency and evacuation procedures.

Compliance

POL.PPD.010: 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 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, such as in response to a security incident or change in the Government Response Level.

POL.PPD.011: The implementation of all security measures **SHALL** be able to provide evidence that the selection has been made in accordance with the appropriate information security standards ISO27001/27002, Physical Security advice taken from the Centre for the Protection of National Infrastructure (CPNI), and [Government Functional Standard - GovS 007: Security](#).

POL.PPD.012: 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 **SHALL** be subject to annual review, or more frequently if warranted.

Physical security advice

Physical security advice can be obtained by contacting [MoJ Group Security](#).

Security in the office

This document is a summary of the key security points for working in a Ministry of Justice (MoJ) location.

Related information

[Clear screen and desk](#) on page 125

[Mobile Device and Remote Working Policy](#) on page 23

[Passwords](#) on page 105

[Physical Security Policy](#) on page 113

[Remote Working](#) on page 26

[Removable media](#) on page 94

[Reporting an incident](#) on page 14

[Working securely with paper documents and files](#) on page 98

Clear desk and clear screen policy

- Lock away information securely when not in use.
- Where you have visitors or non-security vetted guests, please ensure they are not able to see your work, either hard copy or on your computer screen.
- Always use a privacy screen.
- Be mindful of being overseen from outside. Position computer screens so that they cannot be seen by anyone looking in. Ensure that whiteboards are cleaned at the end of meetings, and cannot be read from outside the building while in use. Ensure that noticeboards cannot be read from outside the building.
- Where there is insufficient lockable storage space, you **SHALL** secure the premises where sensitive information or documents are held. If you are uncertain, talk to your manager.

More information is available in the [clear screen and desk guidance](#).

Ensure your privacy

- Make sure that your private conversations are indeed private, and cannot be overheard by anyone else, especially if you are not in an official work environment.

Removing equipment or hard copy information from MoJ offices

- If you are planning to remove or take information out of an office, whether on IT equipment or removable media, or as hard copy, consult your line manager.
- If you have concerns about the risk of overlooking or overhearing from neighbouring buildings, ask for help: security@justice.gov.uk.

Security keys and combination locks

Compromising a security key or a combination setting may have more widespread effects than the loss of a document. Here are some basic rules.

- 'Scramble' combination locks by turning the dial anti-clockwise at least five times.

- Ideally memorise the combination setting, but if you must keep a local record, make it cryptic and store it in a secure location. Treat the combination like a [password](#) and protect it accordingly.
- Forward a written cryptic record of the settings of combination locks for secure cabinets or safes (but not key safes) to security@justice.cg.gov.uk. For example, you might conceal the combination within a telephone number.
- Change combinations at least every 6 months. Always change the combinations whenever a staff member who knew the combination leaves.
- Always report the loss or compromise of a security key or code immediately using the [security incident reporting arrangements](#).

Protecting equipment

- If you use IT equipment away from the office, do so in accordance with the [Mobile Device and Remote Working Policy](#).
- Lock all portable equipment such as laptop computers away when not in use. Do not leave equipment unattended on desks or in unlocked cupboards.

Remote working

For further guidance on working outside of the office environment, refer to the guidance in the [Mobile Device and Remote Working Policy](#).

Contact details

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

Security threat level and emergency procedures

To keep us all safe, security measures and threat levels are continuously under review. The latest information on changes to our current threat level and emergency procedures can be found below. We encourage you to stay informed and take note of the ways you can help to keep yourself and others safe.

Information for staff

The threat level for international terrorism in the UK is currently (December 2021) at SEVERE. This means that a further attack is highly likely.

The response level across the government estate is currently at HEIGHTENED. This means there is no perception that the threat has altered, but it remains under review.

If you become aware of an incident that threatens the physical security of Ministry of Justice (MoJ) staff or premises:

- In situations that present an immediate threat call MoJ Group Security on 07583035594, including out of hours (24/7).
- In non-urgent cases, create a [security incident report](#), and email it to security@justice.gov.uk.
- Dial 999 in an emergency.

We are constantly reviewing our security operations and contingency planning across the MoJ estate. It is essential that staff support us by remaining vigilant and cooperating with [security policies](#).

You can help by [reporting any suspicious behaviour around MoJ buildings](#), for example cars parked strangely or moving slowly, or people observing, loitering or asking unusual questions.

Wear your pass at all times within the building, and challenge those without one. Never wear your pass outside, as it draws attention to you as a civil servant.

View our [top tips for keeping the MoJ safe](#) for further information and our [counter-terrorism intranet page](#).

Contact details

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

Visitor Access Policy

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

This Visitor Access Control and Escorting Policy 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.

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

Objective

This policy outlines the access and security management controls that are in place for all visitors to MoJ buildings, along with requirements to be completed for escorted or unescorted visitors.

Scope and Definition

For the purpose of this policy, visitor control and escorting procedures are physical security controls that are intended to protect the MoJ from those wishing to gain unauthorised access or cause surreptitious or forced attack.

POL.VAP.001: Government organisations **SHALL** have mechanisms to implement internal and external security controls in a layered fashion that deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive, against forcible or surreptitious attacks.

Context

POL.VAP.002: The work of the MoJ involves a level of risk that is susceptible to physical threats, including crime and national security threats such as terrorism and espionage. Security risks **SHALL** be managed effectively, collectively and proportionately to achieve a secure and confident working environment.

POL.VAP.003: The MoJ **SHALL** implement effective and proportionate security controls to reduce physical risks (including crime, natural hazards and terrorism) to our assets (people, information and infrastructure) to an acceptable level.

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.

POL.VAP.004: Staff **SHOULD**:

- Comply with the visitor access procedure when sponsoring a visit.
- Notify the MoJ of any [foreign delegates or visitors](#) well in advance of the visit taking place.
- Advise visitors of any requirements they need to fulfil prior to the visit, including providing confirmation of clearance if required, and bringing [valid ID](#). Inform them of any searches they **MAY** be subjected to.
- Inform colleagues of any expected visitors.
- Ensure that a visitor categorised as requiring an escort **SHALL** always be accompanied by a member of staff.
- Challenge any escorted visitor found to be unaccompanied and seek assistance if required. The unescorted visitor **SHOULD** be returned to reception.
- Ensure visitors remove their pass when leaving the building and that they return the pass to reception at the end of their visit.
- Be mindful of any sensitive conversations that might be subject to unauthorised overhearing. Staff **SHOULD** hold such conversations away from any visitors.
- Ensure that visitors do not have access to any sensitive or high profile areas of the business, unless specifically authorised. Where such access is authorised, staff working in these areas **SHOULD** apply more stringent controls to avoid disclosure of any information.

- Be aware that noncompliance with hosting duties is regarded as a breach of security.

Policy Statements

POL.VAP.005: The MoJ **SHALL**:

- Put in place arrangements to control and monitor access to our estate, including Visitor Control and Escorting policy.
- Have effective plans or procedures in place for dealing with and intercepting unauthorised visitors, intruders or suspicious items. These plans **SHALL** include the ability to search and cordon off areas of the establishment systemically.

This policy has been tailored to reflect the outcomes detailed in [Government Functional Standard - GovS 007: Security](#), and sets out the processes to be completed when organising and overseeing visitor access to the MoJ estate.

Determining Visitor Access Controls

POL.VAP.006: MoJ Estates should refer to the government response levels and their individual threat assessments to determine the level and appropriate visitors control required to manage the security risks to their estate. These controls **SHOULD** form part of a layered defence approach.

POL.VAP.007: For high risk estates which contain sensitive information or other valuable assets, there **SHOULD** be a robust pass system to identify the type of visitor and a sign-in procedure. The use of x-ray scanners and searches to minimise the risk of unauthorised and external access to the estate **SHOULD** also be considered.

Visitor access procedure

Note: The MoJ uses two colours to distinguish visitor passes. A **red** visitor pass means that the visitor requires escorting by an authorised MoJ individual at all times, and in all locations within the MoJ premises. A **green** visitor pass means that the visitor does not require escorting while on MoJ premises.

POL.VAP.008: The following procedures **SHOULD** be implemented and followed to manage visitor access appropriately:

- POL.VAP.009: Provide at least 24 hours' notice of any planned visits to MoJ premises.
- POL.VAP.010: If visitors arrive without notice and cannot provide the name or telephone number of the person they are visiting, security **SHALL** refuse them entry to the building.
- POL.VAP.011: All visitors **SHALL** be sponsored by a MoJ permanent member of staff (Civil Servant) who assumes full responsibility for the visit. Clearance checks **SHOULD** be conducted if required, for example when unescorted passes are required. Confirmation of clearance is required for those buildings which specify a minimum clearance requirement.
- POL.VAP.012: Hosts **SHALL** always accompany **red** escort pass visitors when inside the building. If colleagues see a holder of a **red** escort pass visitor without an escort, the visitor **SHALL** be escorted back to reception, who **SHALL** contact the host and ask them to collect their visitor.
- POL.VAP.013: Hosts are responsible for ensuring that **red** escort pass visitors are escorted back to reception and return their pass. Hosts **SHOULD** also remind the holders of **green** unescorted passes to return their pass to reception when leaving the building at the end of their visit.
- POL.VAP.014: Hosts are responsible for advising their visitors to clearly display their pass at all times whilst inside the building, and that they **SHALL** remove and conceal their pass when outside the building.
- POL.VAP.015: Hosts are responsible for the health and safety of their visitors, and **SHOULD** brief them on the MoJ evacuation and invacuation procedures.
- POL.VAP.016: Visitors from Other Government Departments (OGDs) **SHALL NOT** act as hosts in MoJ buildings.
- POL.VAP.017: Holders of either a valid HMCTS or HMPPS pass **MAY** request a **green** unescorted pass from reception. There is no need to arrange visitor access or have them met in reception, but security **MAY** request further identification.
- POL.VAP.018: Civil Servants from OGDs who hold a Common Civil Service Pass (CCSP) **CAN** be issued with a **green** unescorted pass, but security **MAY** request further identification.
- POL.VAP.019: Contractors from OGDs who hold a CCSP and a national security vetting at CTC, SC or DV **CAN** receive a **green** unescorted pass, but security **MAY** request further identification.

- POL.VAP.020: Contractors from OGDs who hold a CCSP at BPSS **MAY NOT** use their CCSP to access MoJ building. They **SHALL** be treated as visitors.
- POL.VAP.021: Searches, including the use of scanners where available, **SHOULD** be considered for all visitors. [Annex B](#) provides additional guidance and policy statements for accommodating the religious obligations of Sikh visitors.
- POL.VAP.022: For health and safety purposes, a register **SHOULD** be maintained by reception to record the details of the visitor. This applies to security manned sites only. The register **SHOULD** include the visitor name, host unit or contact, date and time of entry, date and time of departure, and a contact number.
- POL.VAP.023: Visitor passes are exclusively for the use of visitors. Contractors or consultants working for and paid by the MoJ are not visitors, and therefore **SHALL** be security cleared before starting work at or for the Department, and issued with a valid building pass. In the rare case of an individual being employed on a very short-term contract not involving access Departmental assets or information, the business unit **SHALL** approach [MoJ Group Security](#) beforehand to obtain approval for the usual clearance requirements to be waived for specific individuals on specific dates.
- POL.VAP.024: Visitor passes are intended for temporary use only, and **SHALL NOT** be used as permanent means to allow for routine daily escorted or unescorted access to the MoJ estate.
- POL.VAP.025: A visitor's pass **SHALL NOT** be used as a substitute or way to circumvent the issuing of a permanent building pass.
Note: This does not include waiting for the replacement of a lost or stolen pass.
- POL.VAP.026: Where a staff member or contractor has forgotten their building pass on the day, they **CAN** be issued with a temporary **green** unescorted visitor day pass, on the proviso that another member of staff can vouch for them. If a staff member or contractor has forgotten their pass on two or more consecutive days, the pass **SHALL** be deemed lost or stolen. The staff member or contractor **SHALL** report to building Security Team before issue of a temporary pass is approved.

International delegations or visits

POL.VAP.027: In the case of international delegations visiting the MoJ, advice **SHOULD** be obtained in advance from the [International Relations and Strategy Team](#).

Prisoners on licence visiting MoJ premises

POL.VAP.028: Where it is necessary for any prisoner who is subject to licence conditions to visit MoJ offices, it is the responsibility of the Offender Manager to undertake a thorough risk assessment well in advance of the planned visit. The assessment **SHOULD** be shared with the host. The risk assessment **SHOULD** be referenced by the visit host on their own risk assessment for the visit in question, and shared with [MoJ Group Security](#). Advice on completing risk assessments is available on the [MoJ Intranet](#).

Common Civil Service Pass (CCSP)

POL.VAP.029: Staff from other government departments who hold a CCSP **CAN** access and visit the MoJ building unescorted. They **SHALL** present their pass to reception staff, and are then issued with a **green** unescorted visitor pass.

For further information regarding the Common Civil Service Pass, refer to [Annex A](#).

Other Government Departments or Private Estates

POL.VAP.030: MoJ staff occupying buildings with other government departments or accommodated in privately leased buildings **SHOULD** refer to and follow internal policies and procedures regarding visitor access.

Guarding responsibilities

POL.VAP.031: Security guards **SHOULD** check all passes every time any person enters a secure building via reception. This is a means of identifying the person presenting the pass. It also ensures that the passes have not been lost and possibly fallen into the hands of unauthorised persons who make improper use of them.

POL.VAP.032: When a valid pass is not presented but scanners are available, security **SHOULD** refuse access and direct the individual through scanners and subsequent searches before reporting to reception to obtain a valid building pass.

POL.VAP.033: [Annex B](#) refers to specific entry search procedures that **SHALL** apply for Sikh visitors wearing the Kirpan.

Types of accepted identification

POL.VAP.034: Visitors **CAN** be asked to present ID. The following are the only recognised forms of ID accepted by the MoJ:

- Current passport.
- Current UK or other internationally-recognised driving licence.
- UK Government Department ID as recognised by MoJ Group Security.

Only original forms of the recognised ID are accepted. No copies are acceptable.

Compliance

POL.VAP.035: The level of risk and potential impact to MoJ information, assets and people determines the controls to be applied and the degree of assurance required. The MoJ **SHALL** ensure 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 change in the Government Response Level.

POL.VAP.036: The implementation of all security measures **SHALL** be able to provide evidence that the selection has been made in accordance with the appropriate information security standards ISO27001/27002, Physical Security advice taken from the Centre for the Protection of National Infrastructure (CPNI) and [Government Functional Standard - GovS 007: Security](#).

POL.VAP.037: 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 is subject to annual review, or more frequently if warranted.

Physical security advice

For more physical security advice, contact [MoJ Group Security](#).

Annex A - Common Civil Service Pass Information Sheet

For access to this information, contact mojgroupsecurity@justice.gov.uk.

Annex B - Sikh Visitors

This guidance provides for reasonable accommodation for religious freedoms as defined by United Kingdom Equalities legislation and the Human Rights Act, while clearly identifying the conditions under which the Kirpan may be worn.

Definition of a Kirpan

The Sikh faith follows a dress code which encompasses the 5 Ks. The Kirpan is one of the 5 Ks. As is the case with all faiths, people follow tenets of their faith to different degrees. Not all Sikhs make a commitment to live by the full Sikh religious code. Therefore, not all Sikhs wear the turban or carry the Kirpan. However, all baptised Sikhs (Amritdharis) who live by the code are required to wear all 5 Ks. Both men and women can be baptised, and the code is the same.

The 5 Ks are defined as follows:

1. Kesh: Uncut hair, which includes keeping a beard. Baptised Sikhs have an untrimmed beard which is either rolled up and tied, or free flowing. A turban is usually worn on their heads to cover the uncut hair. Whilst the turban is mandatory for baptised Sikhs, it is considered to be an integral part of the makeup of the Sikh identity and therefore might be worn by many non-baptised Sikhs.
2. Kara: Steel bangle, predominantly worn on the right wrist. Most Sikhs wear a Kara.
3. Kanga: A small wooden comb in the hair underneath the turban.
4. Kachera (or kachh or kaccha): Cotton loose boxer style shorts with a draw string waist.

5. Kirpan: Ceremonial sword. There is no fixed style of Kirpan, and it can be anything from a few inches to three feet long. It is kept in a sheath, which is attached to a fabric belt and can be worn over or under clothing. The Kirpan signifies that the wearer is blessed with honour. The Kirpan is worn by baptised Sikhs only.





Procedures

POL.VAP.038: A Sikh visitor **SHOULD NOT** be denied entry into the building for genuinely wearing any article of their faith.

POL.VAP.039: The previous information about the [Kirpan](#) **SHOULD** be used as a reference guide to enable security guards to satisfy themselves of the visitors' Sikh faith.

POL.VAP.040: There is no requirement for the removal or confiscation of any articles, particularly the Kirpan, and under normal circumstances, guards **SHOULD NOT** ask to inspect items that are not visible.

POL.VAP.041: It **SHOULD** be noted that when a Sikh is required to remove their Kirpan, they must make an immediate visit to the temple for the Kirpan to be blessed. Therefore, Sikh visitors **SHOULD** only be subject to searches and inspections of their Kirpans in exceptional circumstances, where there is a genuine cause for concern to security.

POL.VAP.042: Where a search and inspection are required, guards **SHOULD** note that it might take the Sikh visitor a few moments to pull their Kirpan from underneath their clothes. This could involve pulling the outer clothes out from their trousers and for women this could be more problematic. To accommodate for this, permission **SHOULD** be sought from the Sikh visitor to feel the Kirpan while still underneath the clothes; or to take the visitor to one side to provide some privacy during the search. Female Sikh visitors **SHOULD** be searched in private by a female security guard.

Contact details

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

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](#).

Related information

[Security in the office](#) on page 117

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:

- Avoid leaving files on your desk top where the name might attract attention. For example, having a file on your desk top called `MyPasswords.docx` is a bad idea, for several reasons!
- Avoid having files or information labelled `SENSITIVE` displayed or stored on your desk top.

Clear desk

Users **SHALL** comply with the following:

- Where possible, paper and computer media **SHALL** be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, particularly outside working hours.
- Where lockable safes, filing cabinets, drawers, cupboards, or similar secure storage areas are not available, doors **SHALL** be locked if rooms are left unattended. At the end of each session all `OFFICIAL` and `OFFICIAL-SENSITIVE` information **SHALL** be removed from the work place and stored in a locked area.

- When handling OFFICIAL documents security **SHALL** follow the requirements laid down in the [Government Classification Scheme \(GCS\)](#).
- OFFICIAL or OFFICIAL-SENSITIVE information, when printed, **SHOULD** be cleared from printers immediately.

[Think before you print.](#)

It is good practice to lock all rooms and office areas when they are not in use.

Information left on desks is also more likely to be damaged or destroyed in a disaster such as fire or flood.

Contact details

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

Equipment Reassignment Guide

Introduction

This guide describes how to reassign equipment. It applies to laptops, mobile phones or other Ministry of Justice (MoJ) issued equipment. Reassignment is from one user to another.

Who is this for?

This guidance applies to:

1. **Technical users:** these are in-house MoJ Digital and Technology staff. They are responsible for implementing equipment controls. The controls apply 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.
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, and storing data) for, or on behalf of the MoJ.
3. **General users:** all other staff working for the MoJ.

"All MoJ users" means General users, Technical users, and Service Providers.

Returning Equipment

When a project completes, or a colleague leaves or moves to a new role, equipment no longer required **SHALL** be returned. The Line Manager (LM) is responsible for using the Service Catalogue to request a return of the item. The equipment might then become available for use by other employees. It might not be cost-effective to consider reusing or reassigning the equipment. Possible reasons include:

- Older technology that might have been heavily used.
- The likelihood of operating problems and failures.
- Lack of support, updates, or patches.
- Slower performance.

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 166

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.

Where data should be saved when using a laptop

It is best to avoid saving any data on a laptop hard drive. However, if you absolutely must, you should always remember to copy or move the data to the MoJ network as soon as you next can connect to it, either via secure remote access or by direct connection.

In order to avoid potential data loss, save data in:

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

There is a better chance of recovering lost data if you have saved it to the MoJ network, as data stored on the MoJ network is backed up daily.

The impact of hard drive failures

Hard drive failures can lead to the irrecoverable loss of data. Any data loss can have security implications for the MoJ, and a significant impact on:

- Our business opportunities.
- Our reputation.
- Our ability to deliver services to the public.

If you experience any issues with your laptop or IT service, [ask for help](#).

For more information about the main security issues that are likely to affect remote and mobile workers, refer to the [remote working guide](#).

How to reset your password

To reset your password, you will need to contact the [IT Service Desk](#). They will carry out checks to confirm your identity. This might include asking your line manager or court manager to confirm your identity, by sending an email to the IT Service Desk. Once your identity is confirmed, your password will be reset and you will quickly regain access to your laptop.

General enquiries, including theft and loss

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

- Tel: 0800 917 5148
- [MoJ Service Portal](#)

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

Contact details

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

Locking and shutdown

The Ministry of Justice (MoJ) has made a commitment towards sustainable IT. The intentions are:

- To reduce overall power consumption for the MoJ by switching off machines and saving energy.
- To reduce the MoJ's overall carbon footprint.

Shutting down a desktop computer

- Close all applications.
- Shut down the computer by clicking the 'Start' button at the bottom left hand corner of the screen. Next, click 'Shut Down'.
- A pop-up box will appear with a drop-down box. Select 'Shut Down' and click 'OK'. After a short delay, your computer will automatically shut down.
- Switch off your monitor screen.

The benefits

By switching off our computers at the end of each working day, we are contributing towards being energy efficient and environmentally friendly. We are all responsible for our own Carbon Footprint. So, please switch off your PC

monitor along with your desktop computer at the end of each working day. In addition, please switch off any other PC monitors if you notice they too have been left on overnight.

Dealing with issues preventing you from switching off your computer

If there are any issues preventing you from switching off your desktop computer overnight, then please raise this with the [IT Service Desk](#) immediately as there could be an underlying fault that needs resolving.

If you require any further information regarding this policy, [ask for help](#).

Locking your computer sessions

Access to most computer systems is controlled by a user name and password. If you have the correct information, you are able to 'log in' or 'log on'. The user name identifies the user as a valid user of the system and the password authenticates that the user is who they say they are.

You are responsible for what you do with an MoJ system or service. You might be held responsible for any actions carried out using your user name and password. You must therefore not allow any one else to do work on any system using your user name and password. If you leave your computer logged on when you are away from it, it might be possible for sensitive information held on the computer system to be used, read, changed, printed or copied by someone not authorised to access it.

If you are leaving your computer unattended for a short period of time, 'lock' the computer by activating the password protected screen saver or similar 'locking' facility. A simple and quick way to lock a Windows computer is:

1. To LOCK - press the Windows key and L key, at the same time.
2. To UNLOCK - press the Ctrl, Alt and Delete keys, at the same time, then log in as normal.

A simple and quick way to lock a Mac computer is:

1. To LOCK - press the Ctrl, Cmd and Q keys, at the same time.
2. To UNLOCK - move the mouse or press any key, then log in as normal.

Laptops

All MoJ laptops have hard disk encryption installed. This protects the entire contents of a laptop's hard disk drive to prevent any data stored locally from being accessed in the event the laptop is either lost or stolen.

Laptop incidents

Investigations into security incidents indicate that a common reason for problems is where the correct security procedures are not being followed. For example, laptops are being left logged on overnight.

This is not good security practice.

If a device is lost or stolen whilst the machine is in locked mode, the data on the machine is more vulnerable to a potential security breach.

Leaving the laptop in MoJ premises is not sufficient to guarantee the equipment's security. Laptop losses do sometimes occur within MoJ offices. There is a greater risk of data loss when a laptop is left partially logged on overnight, so you should always fully log off the laptop at the end of your working day.

Laptop security

- Switch off the machine completely at the end of each usage.
- Do not attach the password to the machine or keep the password with the machine.

If you need further assistance or information about this process, [ask for help](#).

General enquiries, including theft and loss

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

- Tel: 0800 917 5148

- [MoJ Service Portal](#)

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

Contact details

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

Policies for MacBook Users

Any User of an Ministry of Justice (MoJ)-supplied MacBook must ensure they comply with this policy, to ensure that security is not compromised when using these devices.

These Policies are supplementary to the GOV.UK and MoJ Enterprise policies, procedures and guidance.

If you are unsure about any of the requirements or content, [ask for help](#).

Policies

- You must not share your login details or password with anyone under any circumstances.
- You must change your password if you suspect it has been compromised, or if instructed to do so by your line manager or other authorised individual.
- You must not attempt to access any other person's data unless you have been authorised to do so.
- You must only collaborate with authorised personnel.
- [Get help](#) if you are subjected to any security incident, or suspect you might be.
- You must logoff or lock your computer when leaving it unattended.
- You must keep your MoJ Digital & Technology equipment close to you and in sight at all times when in public areas.

Top things to remember

You are responsible and accountable for the security of your MoJ equipment at all times.

If you don't think you should do something, you probably shouldn't. If in doubt, [always seek advice](#).

General enquiries, including theft and loss

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

- Tel: 0800 917 5148
- [MoJ Service Portal](#)

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

Contact details

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

Operations security

Protection from malware

Ransomware

Ransomware is a type of malicious software created or used by cyber criminals. It prevents people or businesses from accessing their own data. The software takes hold of the data, holding it "hostage", until a ransom payment is made to release it.

A useful information leaflet is available for download [here](#).

Preventing Ransomware from taking hold of information

- Store all your information in official Ministry of Justice (MoJ) systems. This is general best practice, and also minimises the risk of the data being accessed by the hackers.
- Use a secure antivirus and firewall software. All official MoJ systems have these installed as standard.
- Use a trustworthy VPN when accessing public networks through wifi, for example when working remotely in a coffee shop. All official MoJ systems have a suitable VPN installed as standard.
- Ensure your laptop computer is updated regularly. All official MoJ systems do this for you automatically, as standard.
- Use multi-factor authentication (MFA) methods. Most MoJ systems support MFA, but you might have to enable it yourself.
- Do not provide any personal information to unknown contacts.
- Avoid insecure apps or websites.

Things to look out for if you suspect you have become victim to a ransomware attack

- Unable to open documents.
- Suspicious file names. Files encrypted by ransomware tend to end with `.crypted` or `.cryptor`, rather than the more typical names such as `.docx`, `.pdf`, or `.jpeg`.
- An unrecognised pop-up screen prevents access to your computer.

What to do if you think a ransomware attack is affecting your system

In the event of a ransomware attack, or if you have suspicions one may be taking place, the first thing to do is to [contact your local IT Service Desk](#).

With your help, the IT team attempt to determine which systems have been impacted, and can isolate them immediately. You might be asked to disconnect all your devices from the network or wifi connection, to prevent a further spread of attacks throughout the business.

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:

**Technology Service Desk - including DOM1,
Quantum, and the Digital & Technology Service Desk**

Tel: 0800 917 5148

Note: The previous `itservicedesk@justice.gov.uk` and `servicedesk@digital.justice.gov.uk` email addresses are no longer being monitored.

HMPPS Information and security

- Email: informationmgmtsecurity@justice.gov.uk

- Tel: 0203 334 0324

For non-technology incidents, contact the MoJ Group Security Team: mojgroupsecurity@justice.gov.uk

Contact the Privacy Team for information on Data Protection Impact Assessments: privacy@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.

Control of operational software

Guidance for using Open Internet Tools

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

This guidance gives you:

- An [overview](#) of Open Internet Tools (OIT).
- A [quick checklist](#) to help you decide if you can use an OIT.
- Reasons why you [might](#), or [might not](#), want to use an OIT.
- Things you [must think about](#) when using an OIT, such as [data protection](#).
- Information on [who to contact](#) if you would like help or advice.

Note: To access some of the links in this guide you'll need to be connected to the MoJ Intranet.

Overview

Open Internet Tools (OITs) are applications or services from suppliers outside the MoJ. They often have the following characteristics:

- they are general purpose. This means they are not specific to the MoJ. Other organisations can use them
- they are accessed using the Internet, usually through a web browser. This means that if you have Internet access, you are able to connect to the tools
- they have a basic 'free-to-use' version. This means that you are able to use some or all the capabilities, but with some constraints. For example, an online word-processor might limit you to 5 documents in your account
- they have one or more 'paid for' versions. By paying for the tool, you unlock some or all the constraints

Quick checklist

To help you decide if you can use an OIT to work on an MoJ task, consider the following questions:

- is the task information subject to specific rules or requirements in your part of the MoJ?
- is the task information classified as anything other than OFFICIAL or OFFICIAL-SENSITIVE?
- does the task information include any data identifiable as being about someone?
- is this the first time anyone has used the tool for MoJ business?
- does the tool need access to your account or other data you can access? For example, does it ask to use your MoJ Google or Microsoft Office account?
- does the tool install a web-browser extension?
- is the tool a plug-in for existing OITs we use, such as Slack, Confluence, or Jira?
- could there be damaging consequences if the task information you work with using the tool is:
 - lost
 - stolen
 - published in the media
- are you prevented from exporting all the data from the tool?

- are you prevented from deleting all the data from the tool when you finish working on the task?

If the answer to *any* of these questions is "Yes", you might not be able to use the OIT.

When you have all the answers, request formal approval to use the OIT from your [Line Manager](#). Do this *before* using the OIT.

Why OITs are an opportunity

OITs offer some significant advantages for you and the MoJ, including:

- enabling you to work the way you want to, more effectively
- usually cheaper than buying or building and supporting a dedicated tool
- no need to build or support the tool
- good use of open standards, such as file formats
- reduced need to have specific hardware or software on computers
- rapid patching to address security issues
- easy updates and deployment of new features
- a large pool of help and support
- easy access, whenever you have a network connection
- increasing availability of some or all capabilities when disconnected from the network

Why OITs are a risk

OITs also pose some threats or risks, including:

- dependency on the tool and supplier
- security of access to the tool
- security of information stored within or processed by the tool
- potential difficulty of enhancing or customising the tool for MoJ-specific requirements

But as long you consider the threats or risks, and address them, OITs provide many benefits for you and the MoJ.

Summary

With careful use, OITs help you to work more effectively and efficiently. Think about them as serious and preferable options for performing tasks.

Using OITs

This guidance helps you:

- understand the conditions or constraints that apply to a tool, or a task performed using a tool
- identify and address threats or risks posed by a new tool

Privacy and personal information

Data protection legislation makes you responsible for personal information you work with. You must keep it safe and secure. In particular, you must follow data protection obligations. These include the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Don't use OITs for storing personal data until you have addressed the need to get consent first. Check if using the OIT might need an update to existing privacy policies or notices. Don't use OITs if unlawful disclosure of the information they process might cause damage or distress.

Data protection legislation might also limit *where* you can process personal data. An OIT should have a privacy statement that describes where it stores or processes data. Be ready to contact the OIT provider for more information about this aspect of their service.

Be sure you can fulfil your data protection responsibilities when using an OIT. It might be helpful to complete a [Privacy Impact Assessment \(PIA\)](#).

Complying with personal information requirements can be complex. Don't hesitate to ask for advice: privacy@justice.gov.uk

Classification and security

An OIT can only store or process information [classified](#) at OFFICIAL level.

Think about the MoJ information you work with. What would happen if you lost it, or it's stolen, or published in the media? Suppose the information was overheard in a cafe, or read from your screen on a crowded train. Could there be damaging consequences? If the answer is "No", then it's probably OK to use OITs to store or send that information.

Think also about information moving across the Internet. The data might be safe within the MoJ and in an approved OIT. But what about the connection between the two? Sending information might involve insecure networks.

Be aware of the security implications. Check that enough suitable security measures are in place to protect the information. For example, check for encryption of network connections using [SSL/TLS](#). A simple way to do this is to look for the secure connection indicator in your web browser:



You have a duty of confidentiality and a responsibility to safeguard any HMG information or data that you access. This is [Principle 2](#) of the Government Security Classifications. The MoJ trusts you to work with OFFICIAL information. In the same way, you're trusted to make a reasoned judgement about whether it's safe to use an OIT.

Useful help for deciding what is OK is in [existing social media guidance](#). While it's more about how to act online, the principles are helpful for OITs.

Remember that it is impossible to delete information after it's released in public.

For more information about MoJ IT Security, look on the MoJ Intranet [here](#).

Storage and data retention

Laws and regulations make the MoJ and its employees responsible for managing information. Some examples include:

- the Freedom of Information Act
- the Data Protection Act and General Data Protection Regulation
- the Public Records Acts

When we receive a request for information, we need to know where we hold all the relevant information. Storing business information on appropriate MoJ systems helps us, because:

- we can provide evidence about decisions
- we understand the information held, and where to find it
- we can transfer records to The National Archives

Always store MoJ information in MoJ systems. If you use an OIT, make sure the key information is also stored in an appropriate MoJ system. Guidance on what you must keep [is available](#). At regular and convenient intervals, transfer the information to an appropriate MoJ system. Do the same when you finish the work. Don't forget to remove any redundant information from the OIT.

Most OITs let 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 [MoJ Information Management Policy](#). There is also help on [responding to requests for information](#).

Service and support

OITs are often intuitive and reliable. But that doesn't mean they are always available and always work as you expect. The MoJ can't provide technical support or ensure service availability for them. Always have another way of working if the OIT is not available for some reason or for any length of time. In other words, don't let an OIT become business critical.

Check the OIT usage agreement to find out more about the service and support available.

Note: The MoJ cannot provide technical support for OITs.

Common OITs

There are already many OITs used across the MoJ. Permission to use an OIT might vary, depending on where you work in the MoJ. For example, some teams must not access or use some OITs, for security or operational reasons.

Note: Check with your Line Manager if you want to use an OIT for your work, *before* you use it.

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.

Getting help

For further help about aspects of using OITs within the MoJ, contact:

Subject	Contact
Classification and Security	MoJ Cyber Security team
Storage and Data Retention	Departmental Library & Records Management Services (DLRMS)
Information Assurance	Compliance and Information Assurance Branch
Personal Data	Disclosure Team

Communications security

Information transfer

Bluetooth

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

Related information

[Personal devices](#) on page 35

Overview

Bluetooth is a very short range wifi technology. In everyday terms, Bluetooth devices can 'talk to each other' if they are very close, for example in the same room. This makes Bluetooth really good for wireless devices, for example a telephone headset, or a mouse or keyboard.

Bluetooth works by 'pairing' devices. This makes it quick and simple to use. The problem is that Bluetooth, and the pairing process, is not very secure. This means that attackers might get unauthenticated access to devices. As

an example, an attacker 'listening' to the Bluetooth connection between a computer and a keyboard could possibly intercept passwords or other sensitive information as the details are typed on the keyboard.

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

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

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

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

Accessibility

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

Contact the Security team by email: security@justice.gov.uk

Bluetooth devices and risks

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

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

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

- Eavesdropping
- Unauthorised access
- Message modification
- Denial of service

- Data exfiltration
- Insecure data transmission
- Phishing

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

Best practices for using Bluetooth

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

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

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

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

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

Some Bluetooth devices allow you to choose whether they are 'discoverable'. For example, on Android 'phones, you can go to the Settings -> Connected devices -> Connection preferences -> Bluetooth visibility or similar. The best advice is to change the Bluetooth settings to not discoverable if you can. Only make the device discoverable when you need to connect to a trusted device.

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

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

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

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

Contact details

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

Email

Overview

This document provides you with guidance for safe and secure use of email within the Ministry of Justice (MoJ).

In general, always use email in an [acceptable way](#).

In particular:

- Never circulate messages or material that contains obscene, profane, inflammatory, threatening, harassing (racially, sexually or otherwise), and disruptive, or otherwise offensive language.
- Don't use email or other messaging systems for trivial debates or exchanges with an individual or group of people.
- Don't use MoJ email or other messaging systems for anything other than appropriate business purposes.
- Don't make statements that defame, slander or lower the reputation of the MoJ, any person or organisation.
- Don't forward email [chain letters](#) to your contacts. Instead, report them to security@justice.gov.uk.
- Be aware of unsuitable attachments, for example video clips, images, or executable files. MoJ email automatically filters many unapproved attachment types, particularly those that can contain executable files. Emails containing those attachments are likely to be quarantined and not delivered.
- Avoid excessive use of email, and sending email to large numbers of recipients. Ask yourself if it really makes sense to "Reply All"?
- Any recipients in the "To" or "Cc" fields can retrieve the addresses of all other recipients in those fields. If you are sending an email to a list of people outside MoJ, where privacy of individuals might be relevant, place your list of recipients in the "Bcc" field and set the "To" field to your own address. This ensures that none of the recipients can retrieve the identities of the other recipients.
- Keep your operating systems up to date to prevent susceptibility to viruses.
- Scan email attachments to detect viruses and other malware.

Be aware that the MoJ monitors the use of electronic communications and web-browsing. Your manager can request reports detailing your activity if they suspect inappropriate use of email or web-browsing facilities.

[Ask](#) if you want further information.

Monitoring

The MoJ monitors all email for security purposes.

Specifically, communications may be monitored without notice and on a continual basis for a number of reasons including compliance with legal obligations, effective maintenance of IT systems, preventing or detecting unauthorised use or criminal activities (including cyber-intrusion), monitoring of service or performance standards, providing evidence of business transactions, and checking adherence to policies, procedures, and contracts.

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

Email threats

Although email is a powerful business tool, it has problems. In this guidance, we describe some of the problems, and how you can avoid them.

Email threats often use familiar email addresses to disguise attacks, or to pose as valid emails. Email threats are becoming more frequent and pose one of the biggest problems for MoJ systems and services.

There are many possible threats, including:

- Viruses: These can be spread between computers in emails or their attachments. They can make PCs, software or documents unusable.

- **Spam:** This is unsolicited mail sent in bulk. Clicking on links in spam email may send users to phishing websites or sites hosting malware. Often email spam mimics the addresses of people you know.
- **Phishing:** These are emails disguised to look like a legitimate company or bank to illegitimately obtain personal information. They usually ask you to verify your personal information or account details. Often links will direct you to a fake website, made to look like the real thing.
- **Social engineering:** In the context of security, social engineering refers to manipulating people to do something or divulge confidential information. For example, you might get a call from someone pretending to be from a software supplier, claiming that a virus has been found on your PC; they demand personal details before they can remove the virus.
- **Spoofing:** A spoofed email is where the sender (in this case, a criminal) purposely alters part of the email to make it look as though it was from someone else. Commonly, the sender's name/address and the body of the message are made to look as though it was from a legitimate source. It is commonly used to trick the recipient into providing confidential information such as passwords, or to market an online service dishonestly, or to sell a bogus product. Check the real sender of any email you receive if you ever have any doubt or uncertainty. If the sending address is one you don't recognise, do not click on any link contained within the email.

The MoJ scans approximately 14 million messages a month for threats (figures from November 2020). Of these, we might expect to find 1.4 million "spam" messages, 150,000 "phishing" messages, and about 1,000 malware messages (including viruses). Unfortunately, not every virus or spam email will be identified and blocked. The good news is that there are some simple steps you can take to reduce the threat:

- If you are not expecting the email, do not reply to it.
- If you are at all suspicious, do not divulge your details or any sensitive information.
- Avoid opening potential scam emails.
- 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.

Scams

Scams are "get rich quick" schemes. They make claims such as promising your bank account will soon be stuffed full of cash if follow the detailed instructions in the letter or email. In reality, it is an illegal plan for making money.

A typical scam includes the names and addresses of several individuals whom you may or may not know. You are instructed to send a certain amount of money to the person at the top of the list, and then remove that name and add yours to the bottom.

You are then supposed to mail copies of the letter or email to a few more individuals who will hopefully repeat the entire process. The letter promises that if they follow the same procedure, your name will gradually move to the top of the list and you'll receive money.

Other high-tech scams using IT also exist. They might be sent over the internet, or may require the copying and mailing of computer disks rather than paper. Regardless of the technology used to advance the scheme, the end result is still the same.

Scams are a bad investment. You certainly won't get rich. You will receive little or no money. The few pounds you may get will probably not be as much as you spend making and mailing copies of the letter if hard copy.

By their very nature, scams are harassing. Sending such mails using MoJ facilities is prohibited. The misuse of computer resources to harass other individuals or groups is unacceptable. Any person tempted to forward an email scam should familiarise themselves with the HR intranet pages, particularly the section regarding disciplinary action and electronic communications.

Note: Scams also clog up the system and reduce the efficiency of our servers.

How to recognise a scam

From the older printed letters, to the newer electronic kind, scams follow a similar pattern, with three recognisable parts:

- A hook: this to catch your interest and get you to read the rest of the letter. Hooks used to be "Make Money Fast" or "Get Rich" or similar statements related to making money for little or no work. Electronic chain letters also use the "free money" type of hooks, but have added hooks like "Danger!" and "Virus Alert" or "A Little Girl is dying". These tie into our fear for the survival of our computers or into our sympathy for some poor unfortunate person.
- A threat: when you are hooked, you read on to the threat. Most threats used to warn you about the terrible things that will happen if you do not maintain the chain. Others play on greed or sympathy to get you to pass the letter on. The threat often contains official or technical sounding language to get you to believe it is real.

- A request: some older chain letters ask you to send money to the top ten names on the letter and then pass it on. The electronic ones simply admonish you to "Distribute this letter to as many people as possible." They never mention clogging the internet or the fact that the message is a fake; they only want you to pass it on to others.

If it sounds too good to be true, then it is!

Bogus calls

There are a range of scams that can target you at home or at work. Callers usually say they are from IT Support, and tell you that they have detected a virus on your machine that needs to be removed. The bogus caller will then either:

- Direct you to a website, in the hope you will download malicious software.
- Try and obtain details from you about your computer, or the MoJ network.

In all genuine situations, the MoJ IT Service Desk will provide you with an incident reference number if there is a real problem with your machine.

If you receive a call from someone claiming to be from the IT Service Desk, always ensure you ask them for the incident reference number. Then disconnect the call, and call the IT Service Desk yourself, directly. If the original call was genuine, when you provide the incident reference number, they will be able to help you.

In general:

- Treat all unsolicited calls as suspicious.
- If possible, note the details and incoming telephone number of the caller.
- 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 their 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 internet today. Instead of spreading from one computer to another by itself, Good Times relies on people to pass it along.

Sympathy letters and requests to help someone

Requests for help or sympathy for someone who has had a problem or accident.

Urban myths

Warnings and stories about bad things happening to people and animals that never really happened.

Inconsequential warnings

Out of date warnings and warnings about real things that are not really much of a problem.

True legends

Real stories and messages that are not hoaxes but are still making the rounds of the internet.

Traditional chain letters

Traditional chain letters that threaten bad luck if you don't send them on or request that you send money to the top "x" people on the list before sending it on.

Threat chains

Mail that threatens to hurt you, your computer, or someone else if you do not pass on the message.

Scare chains

Mail messages that warn you about terrible things that happen to people (especially women).

Jokes

Warning messages that it's hard to imagine anyone would believe.

Email and storing MoJ information

Data held by the MoJ should be managed in such a way that employees who require the data, for business reasons, can gain access to it. Managers should ensure that data is stored in an area that is easily accessible to those who require access. This includes MoJ information exchanged using email.

If you need further assistance or information about this process, [ask](#) for help.

Accessing emails or information in an absent employee's email account

Staff absences do occur and these can cause disruption to MoJ business where colleagues have no access to relevant departmental information. Staff are away for events such as annual leave, secondment or maternity leave, but they don't make provision for colleagues to access departmental information.

When an absence occurs, there is no right to be able to access another employee's account to obtain information. This is true, regardless of whether the absence is expected or unexpected, for example annual leave or illness.

Accessing another employee's account, without their permission, might contravene data protection legislation.

Data protection legislation protects personal information which relates to identifiable, living individuals held on computers. It specifies that appropriate security measures must be in place to protect against unauthorised access to, loss or destruction of personal data. If you breach this principle you could render the MoJ liable to enforcement action by the Information Commissioner.

Avoiding the problem

If you know you're going to be away for any significant amount of time, you can make life easier for everyone, including yourself, by following these simple steps:

1. Make provision for someone to have access to your work email account during your absence. If you don't know how to do this, [contact your IT Service Desk](#).
2. Create a "handover" package, containing information about the tasks that will, or might, need attention during your absence.
3. Make sure the package has contact details for everyone who might need to help progress or update the status of the tasks.
4. Create an "Out Of Office" notification in your email system; include clear details of who to contact in your absence.

Authorised access to user email accounts

You must not access the email accounts of any other users, unless you are authorised to do so as required by your role. Access is authorised on a case by case basis only, and will typically be aligned to the following circumstances:

- During a criminal investigation by a law enforcement agency.
- During an employee investigation relating to misconduct or a security incident, for example IT misuse.
- Upon the death or unexpected exit of an employee, for example for the retrieval of key information and closing down an account.

Ideally, access will have been organised in advance of an absence. But this is not always the case; sometimes there are unexpected or unusual circumstances. Gaining access in such situations will require substantial escalation to [management and Data Privacy and Security teams](#).

Contacts for getting help

In practice, all sorts of things can go wrong with email from time-to-time. Don't be afraid to [report a problem or ask for help](#); you'll be creating a better and safer work environment.

For general assistance on MoJ security matters, email security@justice.gov.uk.

Suppliers to the MoJ should primarily contact your usual MoJ points of contact.

General enquiries, including theft and loss

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

- Tel: 0800 917 5148
- [MoJ Service Portal](#)

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

General app guidance

When working, you need to communicate with Ministry of Justice (MoJ) colleagues and use business tools ('apps'). You'll also need to work with people outside the MoJ. There are various tools you might use, besides the standard email and telephone tools. This document tells you about the tools you can, and cannot, use for business purposes. This guidance applies to all staff and contractors who work for the MoJ.

Some ALBs, Agencies, or other large groups within the MoJ might have their own, specific guidance regarding how to use certain apps for different purposes.

Access to tools

You can access tools that are provided through your MoJ provided devices by downloading from:

- The Software Centre application on your device (for Dom1 equipment).
- The Self Service application on your Mac (for IT Service Desk managed MacBook laptops).

Currently, access to the tools mentioned in this document is not available from Quantum devices.

For other MoJ provided devices, seek help from your Line Manager in the first instance.

Corporate, work and personal accounts

- A corporate account is for making official MoJ statements and providing official views. Only a small number of authorised people can use it.
- A work account is your normal MoJ account, that you use every day for business as usual. Only you have access to your work account.
- A personal account is your own personal account on gmail, hotmail, yahoo, and so on. You should never use a personal account for business purposes. To be clear: never send your work material to your personal device or your personal email account.

Some of the applications listed make a distinction between general use with a work account, and use with a corporate account. Using a tool with a corporate account means you are providing views or statements on behalf of the MoJ. Never use a personal account for business purposes with any tool.

Remember that if you are authorised to use a corporate account, you are speaking and acting for the whole of the MoJ. When working with a personal account, you are speaking and acting as an MoJ employee and a civil servant.

Always follow all [MoJ policies and guidelines](#) regarding public information, including social media. To access this information you'll need to be connected to the MoJ Intranet.

In particular, follow the [Civil Service Code of Conduct](#).

Using video conference tools safely

The NCSC has excellent guidance on [using video conferencing services safely](#).

Key things to remember *before* a call include:

- Make sure your video conferencing account (or the device or app you are using for video conferencing) is protected with a strong password.
- Test the service before making (or joining) your first call.
- Understand what features are available, for example recording the call or sharing files or screen information.

Key things to remember for *every* call include:

- Do not make the calls public, for example always require a password to join the call.
- Know who is joining the call, in particular check that everyone is known and expected to be present, and that people who have dialled in have identified themselves clearly and sufficiently.

- Consider your surroundings, for example checking what can be seen behind you (forgetting to check information on a whiteboard or noticeboard is an easy mistake).

MoJ Policy and guidance

OFFICIAL and OFFICIAL-SENSITIVE Information

OFFICIAL information is the majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

OFFICIAL-SENSITIVE is not a classification. SENSITIVE is a handling caveat for a small subset of information marked OFFICIAL that requires special handling by staff. You should apply the handling caveat where you wish to control access to that information, whether in a document, email, or other form.

Privacy and personal information (Data Protection)

Some communications tools expect to have a copy of your contacts list. The list is uploaded to the tool server in order to let the tool to function correctly. Think carefully about whether this is reasonable to do. Make sure that sharing your contacts list does not impact any one else's privacy in a negative way.

Data protection legislation makes you responsible for personal information you work with. You must keep it safe and secure. In particular, you must follow data protection obligations. These include the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Complying with personal information requirements can be complex. Don't hesitate to ask for advice:

- Email: privacy@justice.gov.uk
- Slack: #security_privacy_and_live_service_team
- Intranet: <https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/>

Information Management

Many of the tools are only used for your day-to-day communication with colleagues. The information you work with is typically **classified** at OFFICIAL.

Think about the MoJ information you work with when using these tools. What would happen if you lost your mobile device, or it's stolen? Suppose the voice or video call was overheard in a cafe, or read from your screen on a crowded train. Could there be damaging consequences? If the answer is 'No', then it's probably OK to use the tool to communicate that information with colleagues.

You have a duty of confidentiality and a responsibility to safeguard any HMG information or data that you access. This is **Principle 2** of the Government Security Classifications. The MoJ trusts you to work with OFFICIAL information. You're trusted to make a reasoned judgement about whether it's safe to use an approved tool, or whether you should use a different MoJ-provided work tool.

Never send work material to your personal devices or email accounts.

Remember that it is impossible to delete information after it's released in public.

For more information about MoJ IT Security, look on the MoJ Intranet [here](#).

Storage and data retention

Laws and regulations make the MoJ and its employees responsible for managing information. Some examples include:

- Freedom of Information Act.
- Data Protection Act and General Data Protection Regulation.
- Public Records Acts.

When we receive a request for information, we need to know where we hold all the relevant information. Storing business information on appropriate MoJ systems helps us, because:

- We can provide evidence about decisions.
- We understand the information held, and where to find it.

- We can transfer records to The National Archives.

Always store MoJ information in MoJ systems. If you use a tool for work tasks, make sure the key information is stored in an appropriate MoJ system. Guidance on what you must keep is available on the Intranet [here](#). At regular and convenient intervals, transfer the information to an appropriate MoJ system. Do the same when you finish the work. Don't forget to remove any redundant information from a tool by clearing or deleting data if it has been preserved in an MoJ system.

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

Tool name	Tool type	Conditions/ constraints on use	Accessing /installing tool	Audience
Slido	Q&A tool during presentations	Avoid personal or sensitive data	Web browser.	Internal
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)
- [Galaxykey](#) (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 Quantum 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

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.

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.

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. Do one or both of the following:

- Call the IT Service Desk on 0800 917 5148.
- Forward the suspected phish to security@justice.gov.uk with the subject line: 'suspected phish report'.

You can 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.

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 Privacy 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:

**Technology Service Desk - including DOM1,
Quantum, and the Digital & Technology Service Desk**

Tel: 0800 917 5148

Note: The previous
itservicedesk@justice.gov.uk and
servicedesk@digital.justice.gov.uk email
addresses are no longer being monitored.

HMPPS Information and security

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

For non-technology incidents, contact the MoJ Group Security Team: mojgroupsecurity@justice.gov.uk

Contact the Privacy Team for information on Data Protection Impact Assessments: privacy@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 Privacy 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 [MoJ Group Security](#).

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

- Tel: 0800 917 5148
- [MoJ Service Portal](#)

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: POLWIFIxxx, 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.

POLWIFI001: 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

POLWIFI002: 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.

POLWIFI003: Wifi networks **SHALL NOT** be treated as extensions of trusted LANs or WANs.

POLWIFI004: Wifi networks **SHALL** be treated as untrusted bearers for the purposes of application security.

POLWIFI005: All products used in an MoJ wifi network **SHALL** support WPA2-Enterprise.

POLWIFI006: CCMP **SHALL** be used to protect the confidentiality and integrity of information transmitted over the wifi network.

POLWIFI007: Other wifi security modes (such as WEP) **SHALL NOT** be enabled.

POLWIFI008: All products used in MoJ wifi networks **SHALL** support certificate-based authentication.

POLWIFI009: 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.

POLWIFI010: MoJ wireless networks **SHOULD** use a DNS resolver that chains to the [Protective Domain Name Service \(PDNS\)](#) service.

POLWIFI011: All MoJ wireless networking equipment **SHALL** be kept patched and secure, whether connecting to MoJ wifi services or GovWifi.

POLWIFI012: 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.

POLWIFI013: Pre-Shared Keys (PSKs) **MAY** be used for user or device authentication.

POLWIFI014: PSKs **SHALL** be unique per user or device.

POLWIFI015: PSKs **SHALL** only be implemented with prior agreement from the cyber security team

POLWIFI016: PSKs **SHALL** be changed at least once a year.

POLWIFI017: EAP-PSK **SHOULD** be used.

POLWIFI018 : In higher-threat situations such as in a prison location where any unauthorised use of the Wireless network would constitute a security incident, mutually-authenticated authentication based on certificates **SHALL** be used.

POLWIFI019 : EAP-TLS or EAP-TTLS **SHOULD** be used.

POLWIFI020 : Where user or device groups have differing functions, PKI trust domains **SHOULD** be defined and used to maintain functional separation.

MoJ special-purpose wifi networks

POLWIFI021 : If MoJ devices, including IoT or legacy devices, cannot meet the general security policy requirements, or if there are non-security reasons for segregating traffic onto different SSIDs, then dedicated MoJ wifi networks **MAY** be created.

POLWIFI022 : These dedicated networks **MAY** have reduced authentication controls, for example a shared PSK or a reduced ability to rotate PSKs due to form-factor limitations.

POLWIFI023 : In such circumstances, special care **SHALL** be taken to ensure that the general network architecture and other security controls constrain network connectivity for clients. The constraints limit network connectivity to the minimum required for them to function properly.

POLWIFI024 : Other mechanisms such as MAC filtering **SHOULD** be used to reduce the chance of misuse.

MoJ guest wifi networks

Due to complexities and management effort involved in running wifi solutions, the MoJ preference is to utilise the cross-Government GovWifi service: <https://www.wifi.service.gov.uk/>.

This also has the benefit of being available across HMG Departments and Agencies. GovWifi has a level of pre-registration, monitoring and filtering in place to protect the users. However, GovWifi does not provide enterprise level security functions. GovWifi users are required to maintain their own security controls. For MoJ users of GovWifi connections, this means using the MoJ-provided VPN services when accessing protected MoJ services.

POLWIFI025 : Any considerations for not using GovWifi in an MoJ guest wifi network **SHALL** be discussed and agreed beforehand with the cyber security team.

POLWIFI026 : Where GovWifi cannot be used, or where an existing guest wifi service exists, the following **SHALL** be in place:

- Regular rotation of the passphrase, with agreement from the [Security team](#). Normally, this requires a fresh and unique passphrase each day.
- Filtering and Monitoring for known 'bad-sites' and threats **SHALL** be in place at the network level.
- Guests wishing to utilise the service **SHALL** first register for access, and can then be provided with the passphrase for that day.

Logging and monitoring

POLWIFI027 : Security monitoring for MoJ wireless networks **SHALL** be implemented, in accordance with the MoJ security monitoring policy.

POLWIFI028 : Security logging **SHALL** be enabled to record activity such as client access events, authentication successes and failures, client association history, and relevant information about devices and users attempting to connect to the wireless network.

POLWIFI029 : In higher threat environments, security logging **SHOULD** also include identification of rogue access points, and logging of all attempted associations with the wifi network.

POLWIFI030 : 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

POLWIFI031: MoJ staff **SHALL** ensure they have permission from the network owner before using wifi that is not operated by the MoJ.

POLWIFI032: Staff **SHOULD** take [reasonable precautions](#) to check that their home wifi network is secure.

POLWIFI033: Staff **MAY** use work-provided mobile phones to 'tether' their MoJ-provided devices for connectivity.

POLWIFI034: Tethered connections **SHALL** be password protected using unique and complex passwords.

POLWIFI035: Tethering passwords for MoJ devices **SHALL NOT** be shared with non-MoJ users.

POLWIFI036: 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 PTP/MoJO laptops and mobile devices.

POLWIFI037: Staff travelling overseas **SHALL** follow the guidance on [Accessing MoJ IT systems from overseas](#) and [taking equipment 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

Lost devices or other IT security incidents

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

Related information

[Laptops](#) on page 127

What to do if your device is lost, stolen, or compromised

If MoJ data or information is lost or compromised, you should always [report it as a data incident](#).

Note: You can help reduce problems by making sure that devices used for MoJ tasks are always shut down before leaving Government premises. Locking a laptop, or 'putting it to sleep' is not completely secure. A lost or stolen

laptop can be accessed more easily if it is only locked or sleeping. A shut down makes sure that all security measures are in place, such as full disk encryption.

If you think your device is lost, stolen, 'hacked', or in some way compromised, you must:

1. Contact your IT Service Desk. The analyst will ask the relevant questions and note responses on the ticket.

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

- Tel: 0800 917 5148
- [MoJ Service Portal](#)

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.

2. Tell your line manager as soon as possible.
3. For a lost or stolen device, contact the Police and make sure you get the incident reference number.

Summary

Find out more about how to [report a security incident](#).

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 Privacy 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

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.

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.

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.



© Crown copyright 2022

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

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

