Ministry of Justice (MoJ) Cyber Security Guidance: Intranet Edition

Contents

Intranet landing page

This document is an offline version of the security policy and guidance decisions that the Ministry of Justice (MoJ) has made for the products we operate, and our relationships with suppliers.

This guidance is dated: 1 July 2021.

It is time-limited, and is not valid after 1 August 2021.

Equipment

Equipment

The Ministry of Justice (MoJ) uses a variety of devices and services to build and provide its services, and to perform its work.

This information tells you about how to keep the MoJ equipment safe and secure.

Clear screen and desk

Clear Screen and Desk

Users shall comply with the following:

- Digital Services 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 (set to 5 minutes by default). This 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.

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 etc. are not available, doors must 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.

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.

Data and equipment management

Equipment management

You are responsible for looking after the safety and security of Ministry of Justice (MoJ) equipment that you use to do your job.

This information helps you keep MoJ equipment safe and secure.

Bluetooth

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

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 Cyber Assistance Team by email: CyberConsultancy@digital.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

Bluetooth device	Suitable for MoJ work purposes (Y/N)
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

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 see 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 see 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 see 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 see 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.

Contacts

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

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 correspondance 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 Cyber Assistance 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 Operational Security Team and the MoJ Chief Information Security Office (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 (see Data Movement Form, where advice should be obtained from the MoJ Chief Information Security Office (CISO) 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, see 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 Operational Security Team: OperationalSecurityTeam@justice.gov.uk, or CISO on the best option to use when completing the DMF (see 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, be 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 Information Assurance and the MoJ CISO 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 e-mail.

Sharing information above `OFFICIAL`

Where there is a business requirement to share information classified higher than `OFFICIAL`, advice **SHALL** be sought from the Operational Security Team: OperationalSecurityTeam@justice.gov.uk or CISO prior to completing a Data Movement Form.

Data Movement Form (DMF)

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 Senior Information Risk Owner (SIRO).

A DMF **SHALL** be completed, and approval received from the Operational Security Team, for the following scenarios:

- Data is being moved or shared by transferring a physical device, for example using a storage array, USB drive, or other removable media.
- Data is being moved or shared by electronic (network) communication, where the movement is from an MoJ IT system to an external party.

A DMF **SHALL** be submitted to the Operational 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.

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 Operational 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 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 Operational 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 e-mail 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 e-mail 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

DOM1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous `itservicedesk@justice.gov.uk` email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: `#digitalservicedesk`

HMPPS Information & security:

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

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.
- Avoid excessive use of email. Be aware of unsuitable attachments, for example video clips, images, or executable files.
- Avoid sending email to large numbers of recipients. Ask yourself if it really makes sense to "Reply All"?
- 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 e-mail, 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 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 service desk, always ensure you ask them for the incident reference number. Then disconnect the call, and call 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 there friends about some terrible virus that is destroying people's systems? Or help this poor little girl who is about to die from cancer?.

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

The risk and cost of hoaxes

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

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

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

How to recognise a hoax

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

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

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

These make it very difficult to be certain a warning is a hoax. Check to see 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 Helpdesk.
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.

For Cyber Security assistance or consulting, email CyberConsultancy@digital.justice.gov.uk.

Suppliers to the MoJ should primarily contact your usual MoJ points of contact.

General enquiries, including theft and loss

DOM1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous `itservicedesk@justice.gov.uk` email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: `#digitalservicedesk`

HMPPS Information & security:

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

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 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.

Contacts

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

Information classification, handling & 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.

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

Classification	Definition	Marking
OFFICIAL	All information related to routine public sector business, operations and services. Almost all personal information falls within the OFFICIAL classification.	

Classification	Definition	Marking
	OFFICIAL-SENSITIVE is not a separate security classification. It should be used to reinforce the need to know principle, beyond the baseline for OFFICIAL.	OFFICIAL data does not need to be marked except where SENSITIVE, and must be marked OFFICIAL-SENSITIVE.
SECRET	Very sensitive information that requires protection against highly sophisticated, well-resourced and determined threat actors, for example serious and organised crime.	Must be marked
TOP SECRET	Exceptionally sensitive information that directly supports (or threatens) the national security of the UK or its allies and requires extremely high assurance of protection from all threats.	Must be marked

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

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

The consequences of not classifying information correctly are outlined below:

- 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 Cyber Assistance Team (CAT) immediately: CyberConsultancy@digital.justice.gov.uk.

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 Cyber Assistance Team (CAT) immediately: CyberConsultancy@digital.justice.gov.uk.

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 Operational Security Team (OperationalSecurityTeam@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.	
	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.

Type	Measure	Example
TECHNICAL	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.

Type	Measure	Example
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: security@justice.gov.uk.	
	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: security@justice.gov.uk	

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	Handling and storing TOP SECRET information requires exceptional planning, monitoring, and record-keeping.	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.
	Working remotely with TOP SECRET is not permitted due to the extreme sensitivity of the information.	
	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.	
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: security@justice.gov.uk.	

Type	Measure	Example
	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. 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: security@justice.gov.uk.	

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.

Contacts

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

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. See 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 above 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 see 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. See the Knowledge Base article on "How to Re-instate a Deactivated Email Account or Mailbox".

Contacts

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

OFFICIAL, OFFICIAL-SENSITIVE

OFFICIAL

OFFICIAL is a UK HM Government information asset classification under the Government Security Classifications Policy (GSCP).

OFFICIAL-SENSITIVE

OFFICIAL-SENSITIVE is **not** a classification. SENSITIVE is a handling caveat for a small subset of information marked OFFICIAL that require *special* handling by staff above and beyond the described OFFICIAL baseline.

The SENSITIVE handling caveat is a *reminder* as opposed to a requirement for additional controls nor a description of a minimum set of controls.

Guidance on handling OFFICIAL-SENSITIVE data and IT.

DESCRIPTORS

Descriptors *can* be applied (but they do not need to be) to help identify certain categories of SENSITIVE information.

Descriptors should be applied in the format OFFICIAL-SENSITIVE [DESCRIPTOR]

The Cabinet Office maintains the following list of core descriptors to ensure a consistent approach is adopted across all departments:

- COMMERCIAL: Commercial- or market-sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to HMG or to a commercial partner if improperly accessed.
- LOCSEN: Sensitive information that locally engaged staff overseas cannot access.
- PERSONAL: Particularly sensitive information relating to an identifiable individual, where inappropriate access could have damaging consequences. For example, where relating to investigations, vulnerable individuals, or the personal / medical records of people in sensitive posts (e.g. military, SIA).

Descriptors are **not** codewords.

Contacts

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

Personal device use

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

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

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

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

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

Guidance

- If you have an MoJ-issued device or virtual environment, you must use that.
- You must not use a personal device to access Office 365 tools (email, calendar, Word, Excel, Powerpoint, etc.) for work purposes.
- You must not use a personal device to access Google Workspace tools (Gmail, Docs, Slides, Sheets, Drive, Meet, Hangouts, etc.) for work purposes.
- This guidance applies to all tools accessed through a web browser or installed client applications.
- Do not send MoJ information to your personal email account.
- Do not use personal accounts for work purposes.
- Do not store work files or information on a personal device (desktop, laptop, tablet or phone).
- Do not store work files or information on a personal storage device or memory stick (external drive, thumb drive, USB stick, etc.).

- Some teams within the MoJ might have permission to use personal devices for some tasks. This permission continues, but is being reviewed on an on-going basis. Ensure that you have documented approval recording your permission. Ensure that the permission is no more than 12 months old. To request or refresh permission, ask your Line Manager to seek approval by checking with the Operational Security Team: security@justice.gov.uk.

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

Virtual environment

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

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

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

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 worringly, 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 see 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 though 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 & Risk Advisors

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

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 see 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, see the user access page.

Contacts

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

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.

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: OperationalSecurityTeam@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.

Contacts

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

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 Cyber Assistance 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 Operational 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 Operational 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:

DOM1/Quantum - Technology Service Desk	Tel: 0800 917 5148 **Note:** The previous `itservicedesk@justice.gov.uk` email address is no longer being monitored.
Digital and Technology - Digital Service Desk	• Email: servicedesk@digital.justice.gov.uk • Slack: `#digitalservicedesk`
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 Operational Security Team:

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

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

Secure disposal of IT equipment

The Ministry of Justice (MoJ) and its Executive Agencies and Arms Length Bodies use a wide variety of equipment, including desktop computers, laptops, USB memory sticks and other mobile devices. This equipment is procured and managed though MoJ suppliers, who are normally responsible for the secure disposal of the equipment when it is no longer used. Typically, a supplier managed device will have a supplier asset tag on it, making it easier to identify who to ask for help with disposal.

However, there are also other devices 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.

To determine the correct disposal requirement, use the following table to identify the correct outcome, depending on the type of equipment and its security classification. If the table does not cover your exact requirement, contact the Operational Security Team: OperationalSecurityTeam@justice.gov.uk

Note: When disposing of `SECRET` or `TOP SECRET` equipment or materials, always contact the Operational Security Team: OperationalSecurityTeam@justice.gov.uk

Equipment or asset type	Data deletion method	Disposal 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.

Equipment or asset type	Data deletion method	Disposal method
Hard disk drive	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 4 pieces. This can be done either manually or by using a commercially available destruction product suitable for use with hard disks. Alternatively, apply a Lower Level degauss 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	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. A high capacity CD and DVD shredder is available at 102 Petty France, suitable for items up to `TOP SECRET`. Contact OperationalSecurityTeam@justice.gov.uk for help with this option.

Owners of the data storage devices are responsible for procuring services that meet the necessary destruction outcomes as described above. Assurance shall be required that the appropriate destruction has taken place for any locally procured MoJ assets, and that an audit trail is available for inspection upon request by MoJ security.

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

Secure disposal organisations

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

- TYR security: g-cloud@tyr-security.co.uk
- Data eliminate: info@dataeliminate.com

Moving equipment between sites

If you have any concerns about moving items between sites securely, contact the Operational Security Team: OperationalSecurityTeam@justice.gov.uk

Contacts

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

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 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 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 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, Operational Security 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 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 Service Desk via a local or area IT Manager.
- HMPPS Probation - Log an incident with your Service Desk.
- All other teams, contact the Operational Security Team: OperationalSecurityTeam@justice.gov.uk

General enquiries, including theft and loss

DOM1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous `itservicedesk@justice.gov.uk` email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: `#digitalservicedesk`

HMPPS Information & security:

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

Laptops

Laptops

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

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

DOM1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous `itservicedesk@justice.gov.uk` email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: `#digitalservicedesk`

HMPPS Information & security:

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

Contacts

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

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 see 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

DOM1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous `itservicedesk@justice.gov.uk` email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: `#digitalservicedesk`

HMPPS Information & security:

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

Contacts

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

MacBook

MacBook

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

DOM1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous `itservicedesk@justice.gov.uk` email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: `#digitalservicedesk`

HMPPS Information & security:

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

Contacts

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

Incident management

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 cybersecurity nature then use Report a cyber security incident.

Lost devices or other IT security incidents

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

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 Technology Service Desk. The analyst will ask the relevant questions and note responses on the ticket.

   DOM1/Quantum - Technology Service Desk

   - Tel: 0800 917 5148

   Note: The previous `itservicedesk@justice.gov.uk` email address is no longer being monitored.

   Digital & Technology - Digital Service Desk

   - Email: servicedesk@digital.justice.gov.uk
   - Slack: `#digitalservicedesk`
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.

Contacts

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

Remote working

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.

Key points

- Be professional, and help keep Ministry of Justice (MoJ) information and resources safe and secure at all times.
- Think about where you are working, for example - can other people or family see what you are working on? Be thoughtful about information privacy.
- Never send work material to personal email accounts.
- Keep MoJ accounts and password information secure.
- Take care of your equipment. Devices are more likely to be stolen or lost when working away from the office or home.
- Do not leave MoJ equipment unattended.
- Get in touch quickly to report problems or security questions.

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.

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.

Always:

- Keep MoJ equipment and information safe and secure.
- Protect MoJ information from accidental access by unauthorised people.
- Lock or log off your device when leaving it unattended. For long periods of non-use, shut down your device.
- Keep your workspace clear and tidy - follow a 'clean desk policy', including paperwork, to ensure MoJ information isn't seen by unauthorised people.
- Use MoJ IT equipment for business purposes in preference to your own equipment such as laptops or printers.
- Be wary of anyone overlooking or eavesdropping what you are doing.

Never:

- Let family or other unauthorised people use MoJ equipment.
- Leave equipment unattended.
- Work on sensitive information in public spaces, or where your equipment can be overlooked by others.

- Advertise the fact that you work with MoJ materials.
- Take part in conference or video calls when you are in public or shared spaces such as cafes or waiting rooms.
- Send work material to your personal email address.
- Redirect print jobs from MoJ printers to a personal printer.

Working securely

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

- **Work locations** - as with home working above, 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 your own equipment

The main guidance is available here.

Wherever possible, you should always use official MoJ equipment for business purposes. Never send work material to your personal 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. The advice is to avoid printing anything, and in particular not to use personal printers.

However, if you really must print MoJ information, you:

- Should connect directly to the printer using USB, not wifi.
- Should not print out personal information relating to others.
- Should not redirect print jobs from an MoJ printer to a personal printer.
- Should consult the information asset owner or line manager before printing the information.
- Must store any and all printed materials safely and securely until you return to MoJ premises, when they must be disposed of or filed appropriately.
- **Must never** dispose of MoJ information in your home rubbish or recycling.

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 see 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:

- Lock your computer, even when unattended for short periods.
- Think about whether an unauthorised person, such as a family member, might see the information you are working with.
- Don't 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

DOM1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous `itservicedesk@justice.gov.uk` email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: `#digitalservicedesk`

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.

Operational Security Team

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

Privacy Advice

Privacy Team

- Email: privacy@justice.gov.uk
- Slack: `#securityprivacyteam`
- Intranet: https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/

Cyber Security Advice

Cyber Consultants & 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

Overseas travel

Accessing MoJ IT systems overseas

This guidance information applies to all staff, contractors and agency staff who work for the 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.

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 device, and any data the device can access.

Steps to follow before travelling
Part One

1. Get confirmation from your Senior Line Manager that there is a business need for you to take MoJ equipment overseas and access MoJ services. Keep a note of the answers you get.
2. Proceed directly to Part Two of this process below if you are travelling to or passing through one of the following countries:

   Argentina, Armenia, Azerbaijan, Belarus, China (including Hong Kong), Egypt, Estonia, Georgia, India, Indonesia, Iran, Israel, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, the northern area of the Republic of Cyprus, North Korea, Pakistan, Russia, Saudi Arabia, South Africa, South Korea, Syria, Turkey, Turkmenistan, UAE, Ukraine, Uzbekistan.
3. Proceed directly to Part Two of this process below if you are national security cleared to SC or DV levels.
4. If you are subject to STRAP briefing and intend to travel to or through countries not in Western Europe, North America, Australia, or New Zealand, proceed directly to Part Two of this process below, and notify the STRAP team at STRAPTeam@cluster2security.gov.uk.
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. See the International Roaming section below.

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 method of connecting, 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 have received all the approvals, send a copy of your request and the approvals to OperationalSecurityTeam@justice.gov.uk.
7. When Operational Security have acknowledged receipt of the request and approvals, the formal process is complete.
8. Check if you need to do anything to prepare for International Roaming. See the International Roaming section below.
9. Take a copy of this guidance; it includes useful contact details that help in the event of a problem while travelling.

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 Technology Service Desk (see Contacts section below) 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 the Operational Security Team as soon as possible. See the Contacts section below, 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 the Contacts section below.

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 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.

Related pages

- Taking equipment overseas
- Overseas travel
- Staff security and responsibilities during employment

External websites

- Foreign and Commonwealth Office: travel and living abroad

Contacts
Operational Security Team

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

Dom1 - Technology Service Desk

- Tel: 0800 917 5148
- Tel: +44 800 917 5148 from outside the UK, chargeable

Note: The previous `itservicedesk@justice.gov.uk` email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: `#digitalservicedesk`

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

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 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 above steps.
- State that you are carrying official UK government property that is sensitive and that you cannot allow access.

- Ask to see 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 Technology Service Desk immediately and report the device as potentially compromised.

The Technology 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

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

DOM1/Quantum - Technology Service Desk

- Tel: 0800 917 5148

Note: The previous `itservicedesk@justice.gov.uk` email address is no longer being monitored.

Digital & Technology - Digital Service Desk

- Email: servicedesk@digital.justice.gov.uk
- Slack: `#digitalservicedesk`

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.

Operational Security Team

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

Overseas travel

If you are going on a work trip or holiday overseas and you need to take your 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 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 Overseas Travel Guide provides detailed guidance before you travel.

Mobile roaming should be requested via the Service-Now IT Catalogue.

Documents

- 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

- FCO Foreign and Commonwealth Office

Contacts

- Operational Security Team
- MoJ Group Security

Risk assessment

Risk assessment

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.

Contacts

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

Personnel security clearances

Personnel security clearances

Unless otherwise agreed formally by the Ministry of Justice (MoJ) in writing, any person (whether MoJ staff, contractor or through supply chain) who has access to, or direct control over, MoJ data must have satisfactorily completed the baseline.

The Baseline Personnel Security Standard (BPSS) is published on GOV.UK.

National Security Clearances

The MoJ will advise on a case-by-case basis if an individual requires a national security vetting and clearance.

Contacts

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

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.

Contacts

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

Minimum user clearance

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 above 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.

Checking someone's clearance status

To check someone's clearance status, collect the following information:

- Their first name.
- Their last name.
- Their date of birth.

Send this information to the MoJ Group Security Team, by emailing: MoJ Group Security. The team will check with the Cluster, to determine the individual's clearance status, if any. If you are authorised to receive the answer, the team will reply to you with the answer.

Contacts

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

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, see 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, see 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 Oleeo 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 Oleeo.
- 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 Oleeo.
- 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, see 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, see 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, see 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.

Contacts

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

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. See 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, see 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 Oleeo (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 Oleeo.
- 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

See 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, see 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, see 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, see 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, see 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, see 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.

Contacts

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

User access

User access

Acceptable use of Information Technology at work.

This guidance applies to all staff and contractors who work for 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.

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 see 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 a personal account or 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.

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 willful damage to MoJ equipment, should normally be reported to the Police and to the 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 above 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 see 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.

Contacts

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

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.

Contacts

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

Apps

When working from home, you still need to communicate with Ministry of Justice (MoJ) colleagues. 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 Video and Messaging 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 Digital Service Desk (DSD) 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.

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: `#securityprivacyteam`
- 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.

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	Digital Service Desk controlled Mac - Self service, Web browser.	Internal/ External
Microsoft Teams	Communication and collaboration tool: Video and/or voice	MoJ use approved	Dom1 Software centre, Digital 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	Dom1 Software centre, Digital Service Desk controlled Mac - Self service, Web browser.	Internal/ External
Slack	Text messaging, Voice/ Video calls, etc.	Avoid personal or sensitive data	Digital 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
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	External meetings

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 above, please consult our Guidance for using Open Internet Tools and speak to us 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, contact the security team: security@justice.gov.uk.

Other information

Government policy and guidance

GDS Social Media Playbook

NCSC

Video conferencing services: using them securely

Secure communications principles

Using third-party applications

Government Classification Scheme

These summary guidelines are based on The Government Security Classification (GSC) as issued by the Cabinet Office in 2018. The link below provides full handling guidance for information classifications including `OFFICIAL`, `SECRET` and `TOP SECRET`:

https://www.gov.uk/government/publications/government-security-classifications

In summary, the majority of information that is created or processed by the public sector is now classified as `OFFICIAL`. The other two classifications are `SECRET` and `TOP SECRET`.

`SECRET` classification should be used on very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors.

`TOP SECRET` is HMG's most sensitive information requiring the highest levels of protection from the most serious threats.

Classifications can have additional indicators, providing extra information about looking after the information with that classification. A frequently-seen example is `OFFICIAL-SENSITIVE`. This is still classified as `OFFICIAL`, but there is an additional indicator that tells you the information is of a more sensitive nature, and so should be handled and looked after accordingly.

Contacts

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

Open internet tools

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

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.

More information can be found on the MoJ IT & Computer Security pages.

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, contact the security team: security@justice.gov.uk.

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

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.

Contacts

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

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:

- Taking equipment overseas.
- .

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 Operational Security: OperationalSecurityTeam@justice.gov.uk.

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.

Contacts

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

Passwords

This article provides guidance on passwords within the Ministry of Justice (MoJ). It helps you protect MoJ IT systems by telling you about choosing and using passwords. Whenever you see 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 password guidance is for all users.

Best practices for everyone

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.

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 must 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 must 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

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.

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 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 must immediately change the password.

Single-use passwords are time limited. If they are not used within a specific time after generation, they must 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

Contacts

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

Password Managers

Ministry of Justice (MoJ) guidance makes clear that you should have different passwords for different services. These passwords must be complex.

Using LastPass Enterprise

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.

What is a password manager/vault?

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 do you 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.
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.

What makes a good password manager?

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 should I 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 and 1Password are probably the most popular for personal or team passwords. Example password vaults would be Hashicorp Vault, Kubernetes Secrets or AWS Key Management.

For individual use, have a look at LastPass and 1Password. See 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?”.

See also Using LastPass Enterprise.

Contacts

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

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/operation teams but we're working on license funding to make it available to everyone.

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
- if there were any credentials within Rattic that you need access to based on this shared spreadsheet of old Rattic credentials

What it can be used for

LastPass can be used for storing usernames and passwords that are specific to you (for example, your MoJ Google account details).

LastPass can also 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.

Personal use

You could use your MoJ LastPass account to store personal non-work information but as it is a work account belonging to the MoJ you may lose access if you change role and 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 MoJ documents - you must use existing MoJ services such as Office 365 or Google Workspace for that.

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 on the MoJ intranet.

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 overseas 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

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, system 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.

Training and education

Training and Education

The Ministry of Justice (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 they have access to and use. The assets include information, equipment, people and buildings.
- The importance of reporting any actual or suspected security incidents.

Source

Guidance is provided to staff via the Security section of the MoJ Intranet. All new staff starting work within the MoJ will receive mandatory IA training. This should ensure that the new staff member is made aware of their security responsibilities whilst working at the MoJ.