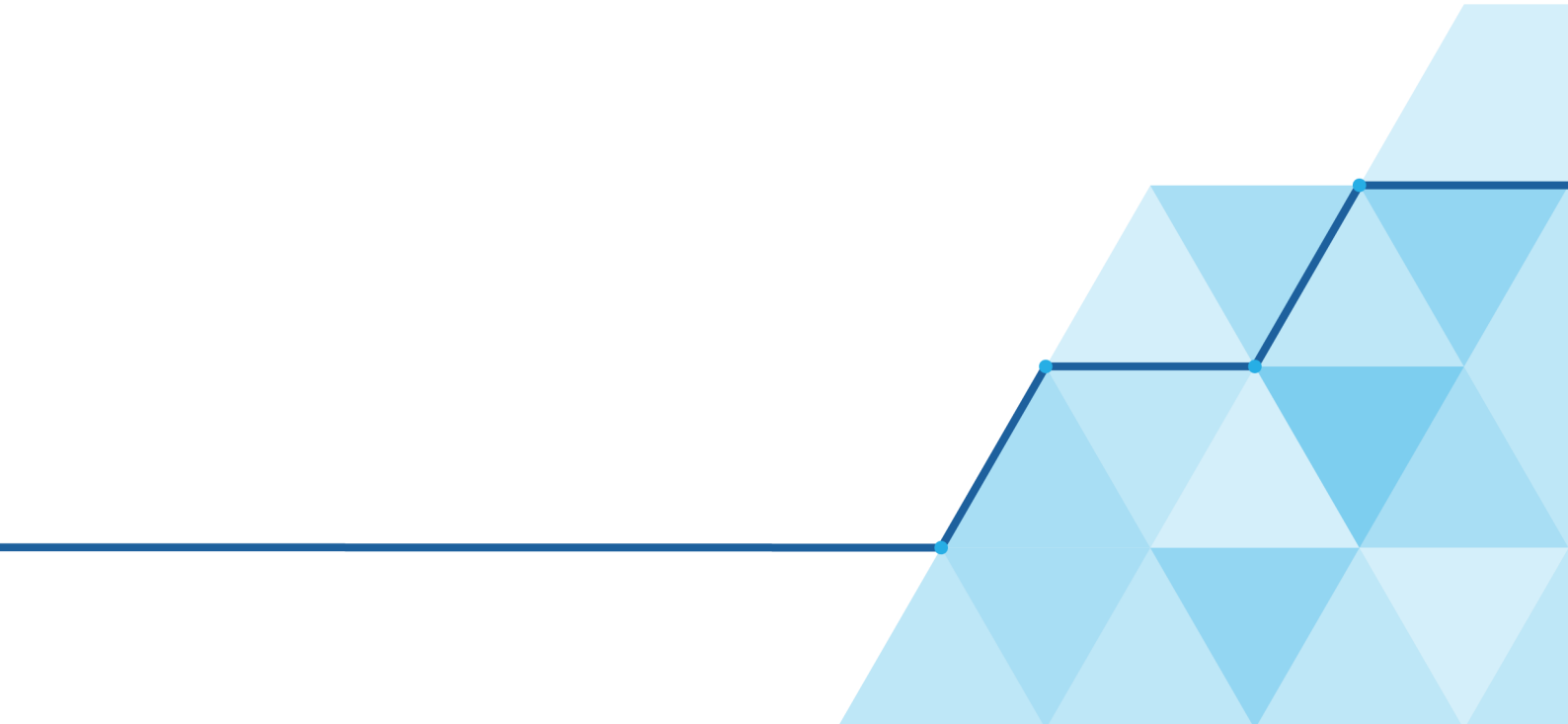
Ministry of Justice

Cyber Security Guidance

Group Security Edition



Contents

Group Security landing page

This document is an offline version of the Group 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: 5 August 2022.

It is time-limited, and is not valid after 5 September 2022.

Contact details

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

Mobile devices and teleworking

Teleworking

Accessing MoJ IT systems from overseas

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

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

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

Essential guidance is provided in the overseas travel information.

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

- Do you need to take MoJ IT equipment overseas or access MoJ IT systems to do your job?
- Can the business need be met in another way or by someone else?
- If you just need to manage your inbox while away, can you delegate permissions to your inbox to a colleague to manage on your behalf?
- Have you left enough time to check and obtain necessary approvals? You should ensure that your request is submitted using the Overseas Travel Form a minimum of fifteen working days before you intend to travel, or if you are subject to STRAP briefing a minimum of twenty working days before you intend to travel. This is because it may be necessary to apply additional technical controls to protect you, your devices, and any data the devices can access.
- Be aware that some countries only consider a passport as valid for a maximum of ten years from its issue date, regardless of the expiry date printed on it. Before travelling, make sure you understand the passport acceptance rules of all the countries you may travel to or through.

Steps to follow before travelling
Part One

1. Get confirmation from your Senior Line Manager (Head of your immediate team) that there is a business need for you to take MoJ IT equipment overseas and access MoJ services. Keep a note of the answers you get.

2. Your Senior Line Manager **should** inform your HR Business Partner (HRBP) of your request to work overseas. The HRBP **shall** advise your Senior Line Manager of any HR considerations concerning your request.
3. If you are subject to STRAP briefing and intend to travel to or through any country not in Western Europe, North America, Australia, or New Zealand, then you **shall** notify the STRAP team at Cluster 2 STRAP team via Security team **and** proceed directly to Part Two of this process.
4. Proceed directly to Part Two of this process if you are travelling to or passing through one of the following countries:

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

Part Two

1. Collect the following information:
   - Name.
   - Email address.
   - Your business area.
   - Your Security Clearance.
   - The network you use to access MoJ data, services, or applications, for example DOM1 or Quantum/MoJO, or online services such as AWS or Google Workspace.
   - The make/type of equipment you want to take with you.
   - Asset Tag details.
   - Countries you'll be visiting or passing through.
   - Dates of travel.
   - Transport details where possible, for example flights or rail journeys.
   - Proposed methods of connecting to MoJ systems or services, for example MoJ VPN, Global Protect VPN (for Macs), wifi, or Mobile Data (3G/4G/5G).
   - Reason for maintaining access while overseas.
   - The MoJ data, applications, or services you expect to access during your trip.
   - Who you are travelling with.
2. The next step depends on your MoJ business area:
   - If you are part of MoJ HQ, HMPPS HQ, HMCTS, or NPS, contact your Senior Line Manager and ask for approval to take MoJ equipment overseas and access MoJ services. Ask for any special details or considerations that apply to your proposed travel arrangements. Keep a note of the answers you get.
   - If you are part of HMPPS (but *not* HQ), contact your Governor and ask for approval to take MoJ equipment overseas and access MoJ services. Ask for any special details or considerations that apply to your proposed travel arrangements. Keep a note of the answers you get.
3. Fill in the Overseas Travel Form.
4. Send the completed form to security@justice.gov.uk, including the answers obtained from the earlier parts of this process.
5. Your request will be considered, and an answer provided, as quickly as possible.
6. When you receive approval for your trip, you might need to schedule a debrief with your line manager or security representative for when you return. Travel approval might be conditional on having a debrief after the trip. If your trip involved visiting a 'special attention' country listed in Part One, a debrief when you return is mandatory.

7. Check if you need to do anything to prepare for International Roaming. Refer to the International Roaming section.
8. **Take a copy of this guidance**; it includes useful contact details that help in the event of a problem while travelling.

On your return

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

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

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

Remain vigilant. In particular, report any approaches or foreign contacts if they occur in the future.

International Roaming

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

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

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

If you have any problem when using MoJ equipment overseas

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

If any security-related incident occurs overseas, regardless of whether it involves MoJ equipment, you should contact security@justice.gov.uk as soon as possible. Refer to the following Contacts section, and the guidance on Reporting a Security Incident on the MoJ Intranet. This includes information on reporting an incident outside of UK working hours. For convenience, the out-of-hours telephone number for reporting incidents is repeated in this guidance.

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

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

Related pages

- General advice on taking equipment overseas
- Overseas travel
- Staff security and responsibilities during employment

External websites

- Foreign and Commonwealth Office: travel and living abroad

Contacts
Security Team

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

IT Service Desk

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

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

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

Information Incident Reporting Line

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

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

MoJ Security

- Email: security@justice.gov.uk

General advice on taking equipment overseas

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

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

General guidance

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

Keeping safe whilst conducting sensitive work overseas

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

- Keep any password/PIN separate from the device.
- Be careful when using your device in situations where it may be lost or stolen, such as busy public places and while transiting customs or security at airports.

- Think about where you are working to ensure that you are not being observed (for instance, somebody looking over your shoulder in a crowded place).
- Never leave the device unattended - not even for a moment.
- If it is not practical to keep the device with you securely at all times (for instance, you are at the swimming pool or gym), consider storing the device in the hotel safe.

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

Guidance on using mobile phones

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

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

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

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

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

If you are on official business:

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

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

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

Contacts for getting help

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

If unsure, contact your Line Manager.

General enquiries, including theft and loss

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

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

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

HMPPS Information & security:

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

Incidents

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

Security Team

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

Overseas travel

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

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

Before you travel on business, you must seek approval from your Senior Line Manager. You **shall** also inform the security team a minimum of fifteen working days (twenty working days if subject to STRAP briefing) before either a holiday or business trip if you are travelling to or through the high-risk countries listed here.

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).

Be aware that some countries only consider a passport as valid for a maximum of ten years from its issue date, regardless of the expiry date printed on it. Before travelling, make sure you understand the passport acceptance rules of all the countries you may travel to or through.

If you are proposing to take MoJ-issued devices with you, or access MoJ systems while overseas, you **should** ensure you comply with the guidance on Accessing MoJ IT systems from overseas.

The MoJ Overseas Travel Guide provides detailed guidance before you travel.

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

Documents

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

Related pages

- Remote working – during COVID-19

External websites

- Foreign, Commonwealth and Development Office (FCDO)

Contacts

- security@justice.gov.uk
- MoJ Group Security

Personal devices

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

Overview

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

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

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

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

Except when connecting to an MoJ virtual environment, or with documented approval in exceptional circumstances as described in this guidance, you **shall not** use a personal device for work purposes.

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

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

Personal devices **shall not** be charged from the USB ports of an MoJ device.

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

Guidance

- If you have an MoJ-issued device or virtual environment, you **shall** use that.
- You **shall not** use a personal device to access Google Workspace tools such as Gmail, Docs, Slides, Sheets, Drive, Meet, or Hangouts for work purposes.
- You **shall not** use a personal device to access Office 365 tools such as Outlook email or calendar, Word, Excel, or PowerPoint for work purposes.
    - Wherever possible, an MoJ work device **should** be used to join business Teams calls, either via video or dial in.

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

Note: You are not asked or required to use your own devices for work purposes. Statement **POL.MOB.009** of the mobile device and remote working policy makes clear that you **should not** use personal devices for MoJ work purposes. If you have access to MoJ devices for work purposes, you **shall** use them by default. A special case is that if you do not have an MoJ-issued mobile phone, you **may** use a personal device to receive Multi-factor authentication (MFA) codes or messages which authorise access by MoJ devices to MoJ systems.

Using MoJ tools on personal devices

In accordance with other policy on the use of personal devices, and the use of mobile devices specifically, you **shall not** use personal devices to access MoJ tools, such as MoJ Slack workspaces.

Note: The rest of this section refers to Slack workspaces, but applies equally to other MoJ tools, such as Teams, Trello, Jira, and so on.

You could of course use personal devices to access other (non-MoJ) Slack communities.

The point is that you **should not** use personal devices for MoJ work purposes. Slack workspaces are official MoJ workspaces and **should** only be accessed using MoJ devices.

Personal devices are not allowed to access services or content containing **Official-Sensitive** data. Work devices **shall** be used to access MoJ services such as MoJ Slack communities. If you do not have a work mobile device, and need to access services such as Slack on a mobile device, you **should** request one using Service Now.

Virtual environment

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

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

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

Connected vehicles

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

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

Additionally, although such platforms usually offer an option to delete paired profiles, there is currently no confirmation that the data is actually erased to a satisfactory level. Transferred information might not be immediately visible or accessible, but this is not the same as deleting the information from the vehicle.

For these reasons, MoJ devices **shall not** be paired with Bluetooth-enabled vehicles.

Contact details

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

Human resource security

Prior to employment

Minimum User Clearance Requirements Guide

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

Security clearance levels

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

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

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

Minimum user clearance requirements

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

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

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

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

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

Please contact the Security team and refer to the National Security Vetting questions for further information.

Contact details

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

National Security Vetting for External Candidates FAQ

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

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

Section 1: Directly employed staff

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

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

If you don't know who your NSVC is, refer to the download here.

Q2. What is the pre-employment check process?

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

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

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

SCS Grades

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

Non-directly employed staff

Refer to Section 2.

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

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

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

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

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

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

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

Non-directly employed workers include the following:

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

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

For posts that require NSV:

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

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

Section 3: National security vetting
Q1. What is National Security Vetting (NSV)?

There are three levels of national security clearance:

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

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

You need the appropriate level of national security clearance if:

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

Q2. How long does national security vetting take?

Refer to Q3, Section 1.

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

If NSV is required for a position, candidates **should not** start until their NSV is confirmed.

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

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

Section 4: National Security Vetting Applications

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

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

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

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

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

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

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

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

Q5. What happens if the candidate misses information out?

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

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

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

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

If you don't know who your NSVC is, refer to the download here.

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

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

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

Section 5: Changes to roles or personal circumstances

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

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

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

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

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

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

For all changes in personal circumstances, please contact Cluster 2 Personnel Risk Management by emailing Vetting team via Security team. Failure to report relevant changes could result in withdrawal of clearance.

Contact details

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

National Security Vetting contact

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

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

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

Roles and responsibilities

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

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

Registration

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

Downloads

The following downloads are available from the MoJ Intranet.

- National Security Vetting contact guide.
- National Security Vetting contact registration form
- National Security Vetting contacts register.

National Security Vetting questions

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

A downloadable version of this document is available here.

National Security Vetting
What is National Security Vetting?

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

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

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

You need the appropriate level of national security clearance if:

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

Can NSV clearance be transferred from another government department?

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

Three scenarios are given here:

Scenario 1: The level of clearance required for the new role is the same level the exporting department held for the individual.	For example, the new role requires SC clearance, and the candidate's exporting department held valid SC clearance for them. Answer: Transfer can take place provided the exporting department confirms a valid NSV clearance **and** agrees to transfer it to the MoJ. In most cases these transfers can take place. In some exceptional circumstances, departments may refuse to transfer clearance to the MoJ. Where this happens, the candidate is required to complete NSV again.
Scenario 2: The level of clearance required for the new role is higher than the level the individual possesses in their current department.	For example, the role requires SC clearance and the current department holds CTC. Answer: As the level of clearance is higher, the employee is required to complete an application for the new level on the NSV portal. A link is sent to them by SSCL once they have accepted a provisional offer.
Scenario 3: The level of clearance required for the role is lower than the current department holds.	For example, the employee currently possesses DV clearance with their present department but their new post in MoJ requires SC. Answer: For security reasons, the MoJ **can not** transfer the higher level of clearance as the **role** does not require it. However, information is extracted to ensure that the candidate is not required to re-apply for a lower level of transfer. This is subject to the current department agreeing to transfer.

Can a candidate start work before applying for NSV?

If NSV is required for a position, candidates **should not** start until their NSV is confirmed.

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

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

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

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

If you don't know who your NSVC is, refer to the download here.

What is the pre-employment check process?

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

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

- All candidates must undergo pre-employment checks relevant to the role, although staff transferring from OGDs have simplified checks.
- SSCL will ask applicants to bring their Right to Work, ID and address documentation to interview.
- Line managers must check these documents, make a note of the document reference numbers and input these into 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, refer to the download here.
- SSCL will only accept requests with a valid vetting reference code provided on the CRF.
- SSCL will send a link to the candidate so they can complete their on-line security questionnaire on the NSVS portal.

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

National Security Vetting Applications
Why are candidates asked to repeat information supplied elsewhere in the recruitment process?

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

What happens if the candidate misses information out?

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

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

How do I check the progress of an application?

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

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

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

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

Changes to roles or personal circumstances

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

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

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

How do I renew NSC?

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

If my personal circumstances change, who do I tell?

For all changes in personal circumstances please contact Cluster 2 Personnel Risk Management by emailing Vetting team via Security team. Failure to report relevant changes could result in withdrawal of clearance.

You can find more information here.

Contact details

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

Pre-employment screening

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

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

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

- Directly employed staff.
- Staff transferring from Other Government Departments (OGD Transfers).

FAQs

- Pre-employment screening and Vetting FAQs

Downloads

- Applying criminal records checks

Contact details

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

Pre-Employment Screening and Vetting of External Candidates - FAQs

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

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

A downloadable version of this information is available here.

Section 1: Pre-employment screening for directly employed staff
Q1. What is pre-employment screening?

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

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

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

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

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

Q2. What is BPSS?

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

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

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

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

If you don't know who your NSVC is, refer to the download here.

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

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

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

- All candidates **shall** undergo pre-employment checks relevant to the role.
- SSCL ask applicants to bring their Right to Work (RTW), ID, and address documentation to interview.
- Line managers **shall** check these documents, make a note of the document reference numbers, and input these into 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

Refer to Section 2.

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

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

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

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

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

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

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

Non-directly employed workers include the following:

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

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

Note: SSCL do not conduct these checks.

Further guidance, and a link to the BPSS Verification Form, can be found on the MoJ Intranet.

If you have posts that require NSV

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

If you don't know who your NSVC is, refer to the download here.

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

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

Section 3: National Security Vetting

Q1. What is National Security Vetting (NSV)?

There are 3 levels of national security clearance:

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

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

You need the appropriate level of national security clearance if:

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

Q2. How long does national security vetting take?

Typical timings from completion of application are

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

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

If NSV is required for a position, candidates **should not** start until their NSV is confirmed.

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

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

Section 4: Applying for NSV

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

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

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

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

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

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

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

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

Q5. What happens if the candidate leaves out information?

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

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

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

If you don't know who your NSVC is, refer to the download here.

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

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

Section 5: Changes to roles or personal circumstances

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

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

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

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

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

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

For all changes in personal circumstances, contact Cluster 2 Personnel Risk Management by emailing Vetting team via Security team.

You can find more information here.

Contact details

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

Security clearance appeals policy

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

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

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

It also applies to:

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

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

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

Policy

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

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

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

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

Further guidance

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

More information about the Security Clearance Appeals Procedures can be obtained from MoJ Group Security.

Contact details

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

Security vetting assessment of need

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

The assessment of need document is available here.

Contact details

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

During employment

Ongoing Personnel Security

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

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

Line Manager Responsibilities

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

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

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

Dealing with concerns

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

When speaking to an individual, remember:

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

Note: For more information, refer to the MoJ Support and wellbeing resources.

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

Managing contractors or consultants

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

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

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

Summary

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

Contact details

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

Personnel risk assessment

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

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

This guidance aims to help risk management practitioners to:

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

Personnel security

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

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

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

Risk management

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

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

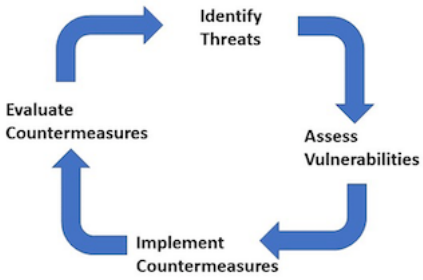


Figure 1: Risk Management Cycle

The methodology defines risk as the product of two factors:

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

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

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

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

The Risk Management process

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

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

Downloads

- Ongoing personnel security: A good practice guide.
- Personnel security risk assessment.

Contact details

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

Reporting personal circumstance changes

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

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

To maintain your security clearance, it is your responsibility to declare relevant changes in your personal circumstances to Vetting team via Security team. Failure to report relevant changes could result in withdrawal of clearance.

You **shall** contact Vetting team via Security team if there is any significant change in your personal circumstances and **shall** alert your line manager or contact the Vetting team via Security team directly if you become aware of any other issue which might increase your security vulnerability.

Please contact Vetting team via Security team if you have any of the following changes to your personal circumstances.

Personal circumstances

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

Personal finances

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

Health, personal problems and aspects of lifestyle

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

Legal matters and involvement with the police

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

Links with extremist or secretive organisations

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

Overseas links or inappropriate associations

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

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

Change of personal circumstance questionnaire

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

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

Changes in circumstances for another member of SC cleared staff

If you become aware of a change in circumstance for another member of security cleared staff, you **should** remind them of their responsibility to report this to Vetting team via Security team.

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

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

- Serious financial problems.
- Substance and drug abuse.
- Alcohol abuse.
- Illegal or injudicious behaviour, including when living or travelling overseas.
- Compulsive gambling.

- Involvement with extreme political groups or inappropriate associations.
- Sexual behaviour is a security concern if it involves a criminal activity, indicates a personality or emotional disorder, subjects the individual to coercion, exploitation, or duress, or reflects lack of judgement or discretion. Sexual orientation or preference are not in themselves disqualifying factors, and are not used as a basis for clearance decisions.

All reports are treated in strict confidence. It is always better to alert a line manager or contact Vetting team via Security team directly, rather than to ignore an issue or take no action.

Contact details

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

Training and Education

Overview

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

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

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

Requirements

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

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

Full details of the mandatory training are provided in the Joiner, Mover, and Leaver pages on the MoJ Intranet.

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

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

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

Further information

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

Contact details

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

Voluntary drug testing policy

Scope

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

This policy **should** be read in conjunction with the Voluntary Drug Testing Policy Procedures.

Purpose

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

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

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

Specifically, it seeks to:

- Minimise the likelihood of existing employees becoming a security concern.
- Implement security measures in a way that is proportionate to the risk.

Government Functional Standard Outcomes

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

Policy Statement

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

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

Voluntary drug testing policy procedures

Introduction

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

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

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

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

If you have any queries about this information, contact MoJ Group Security.

Procedures

These policy procedures support and underpin the Voluntary Drug Testing Policy. Unless otherwise noted, these procedures **shall** be complied with fully.

Aftercare arrangements: Use of Voluntary Drug Testing

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

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

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

Drug testing arrangements

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

Disclosure of personal information

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

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

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

Sample collection

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

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

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

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

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

Raising concerns

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

Confirmation of test results

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

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

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

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

Self-reporting

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

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

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

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

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

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

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

Appealing decisions of withdrawing security clearance

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

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

- Current contractors already engaged on government work in other departments and organisations who have applied for or transferred a security clearance with the MoJ.

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

Appealing a positive drug test

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

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

Review of drug testing arrangements

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

Termination and change of employment

End or change of employment

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

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

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

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

Downloads

Leavers checklist

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

Contact details

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

Leavers with NSC and NSVCs

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

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

If the leaver holds Developed Vetting (DV) or SC enhanced level, and has been STRAP inducted, they **shall** attend a mandatory STRAP debriefing interview with Cluster 2 STRAP team via Security team. They **shall** also sign a confidentiality agreement and a "Declaration of Cessation of **Top Secret** STRAP Access".

NSVCs who leave

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

Manager responsibilities

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

Downloads

- National Security Vetting Contact Guide.
- National Security Vetting Contact Register.
- National Security Vetting Assessment of Need.

Related information

- End or change employment.

Contact details

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

Physical and environmental security

Secure areas

CCTV policy

The policy complements the Ministry of Justice (MoJ)'s overall security policy.

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

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

Objective

The MoJ has in place several CCTV surveillance systems installed within its core buildings. This policy details the purpose, usage, and management of the CCTV systems, and the procedures to be followed to ensure the MoJ complies with relevant legislation and the current Information Commissioner's Office (ICO) Code of Practice.

The MoJ has due regard to the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), the Freedom of Information Act 2000, the Protection of Freedoms Act 2012, and the Human Rights Act 1998. The MoJ also has due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012, and the 12 guiding principles contained therein.

This policy is based upon guidance issued by the ICO.

This policy and the procedures it details apply to the MoJ CCTV systems, including security guards' body worn cameras. CCTV images are monitored and recorded in strict accordance with this policy.

The policy is applicable to all buildings owned or occupied by the MoJ, where MoJ monitored CCTV is installed.

The policy is available for download here.

Contact details

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

Entry and exit search policy

The Ministry of Justice (MoJ) "Entry and Exit Search Policy" applies to all employees, contractors, partners and service providers, including those on co-located sites and sites owned by other public bodies. This also includes employees of other organisations who are based in, or work at, MoJ occupied premises.

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

The policy defines the access controls that are in place when entering and exiting MoJ buildings.

The policy is available for download here.

Physical security advice

Physical security advice can be obtained by contacting MoJ Group Security: mojgroupsecurity@justice.gov.uk.

Contact details

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

Personal mail and parcel delivery policy and procedure

This personal mail and parcel delivery policy applies to all Ministry of Justice (MoJ) employees, contractors, partners and service providers, including those on co-located sites and sites owned by other public bodies. This also includes employees of other organisations who are based in, or work at, MoJ occupied premises.

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

Objective

Following a review by Government Security Centre People and Physical (GSCPP), it is recommended that the MoJ implements a policy on personal and business deliveries, including prohibiting personal parcel deliveries, to MoJ buildings. This policy prohibits deliveries of personal items to MoJ buildings, to comply with HMG minimum physical standard No.10 on mail or delivery management. For further information regarding this standard, contact mojgroupsecurity@justice.gov.uk.

This provides MoJ employees, contractors, partners and other interested parties with a clear policy on mail deliveries, to prevent attack, damage, or interference (malicious or otherwise) to MoJ assets, and - most importantly - physical harm to MoJ people and the public.

Scope and Definition

For the purpose of this policy, personal deliveries are goods purchased over the internet from online retailers or mail subscriptions that are delivered to an office without a legitimate business need. This policy permits vital work-related courier deliveries to reception, as outlined in the policy statement in this document. Vital work-related deliveries are those required to support a business's function, or to support a business need. Ordering gifts to be delivered for colleagues who are leaving the organisation, or for a special occasion, are not considered to be a business-related activity.

Context

The growth in online shopping has seen an increase in the number of personal parcels delivered to the office, as a convenient location because of onsite staff on hand to receive deliveries that would otherwise be returned to depot. However, receiving personal parcels in reception diverts reception and security staff from their core duties, and presents a significant vulnerability to the building's security: the parcel contents are unknown by reception staff. Reception areas are generally within the main fabric of a building and with no separate ventilation or enhanced blast resistant walls, any hazardous substance or explosive device would have a serious impact throughout the building. The MoJ employs off-site mail screening to mitigate against the chances of hostile mail being accepted into MoJ premises.

Couriers often require a receiver to sign a Proof of Delivery document, stating that the parcel arrived in good condition, which risks the MoJ being liable for accepting the package if contents turn out later to be damaged.

Online retailers recognise the needs of their customers of convenience by offering either “Click and Collect” options, or offering parcel collection facilities in convenient locations. This alternative to office-based deliveries is both convenient and reduces the need for staff to carry parcels on their commute home.

Responsibilities

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

Policy Statements

Items required for a legitimate business need **can** be delivered to the office, provided reception have been notified by email from a verifiable email account (for example a Civil Service or Government contractor) 48 hours before the parcel is to be delivered, or as soon as practicable in the case of next-day or same-day deliveries. The email notification **should** provide all of the following information:

- Estimated date of delivery.
- Name of Courier.
- Contact details of the recipient(s), who can sign for the parcel and collect it from reception.

MoJ reception produces a list of scheduled deliveries. Before accepting parcels from the courier, reception confirms who the parcel is for, and that it is a pre-approved delivery. Failure to follow this procedure **may** result in the need to have the parcel scanned, or it being treated as suspicious and the suspicious package process being adopted; disciplinary action **may** be taken.

Compliance

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

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

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

Physical security advice

Physical security advice, including specific advice on this guidance, can be obtained by contacting MoJ Group Security: mojgroupsecurity@justice.gov.uk.

Contact details

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

Physical Security Policy

Audience

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

Physical security is the practice of protecting elements of government infrastructure, estates and personnel against attacks or compromises in the physical (tangible, real-world) environment.

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

Executive Agencies and Arm's Length Bodies (ALBs) are expected to comply with this corporate framework, but might establish their own arrangements tailored to operational needs, and should therefore supplement this policy with local policy or guidance for any business-specific risk.

Objective

This content provides employees, contractors, partners and other interested parties with a clear policy direction. It requires them to ensure that all necessary physical protective security measures are in place to prevent attack, unauthorised access, damage, or interference (malicious or otherwise) to MoJ assets, and most importantly to prevent physical harm to our people and the public.

Scope and Definition

Physical Security refers to measures that are designed to protect physical locations and the assets, information, and personnel contained within.

This policy sets out the approach to be adopted to manage, develop, improve and assure Physical Security across the MoJ.

It is essential that MoJ business is conducted in an environment where potential threats - including those from both natural and human-made hazards, terrorism, crime, and insider threats - to MoJ assets, information, and personnel have been identified, risk assessed and appropriately mitigated to prevent interference, loss, or compromise (malicious or otherwise). This includes ensuring physical perimeters are protected, and entry controls are in place to provide proportionate protection against natural disasters and terrorist attacks.

Context

This policy sets out a framework to follow a "layered" approach to physical security. It provides suitably secure environments from which the MoJ can operate, to achieve its strategic aims and objectives by implementing security measures in layers, to appropriately protect personnel and assets, including material of differing levels of sensitivity.

This policy provides a high-level organisational objective for the MoJ with regards to Physical Security, supported by **mandatory** Physical Security Standards which **shall** be followed to ensure compliance, as they represent the minimum measures required to protect the security of assets, information and people.

Responsibilities

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

The most senior grade based at each site, or in "Moderate Risk" and larger sites the Senior Responsible Officer (SRO), has responsibility for ensuring physical security risk assessments are conducted annually. They **shall** ensure the action plans created to address identified risks and instigate business continuity activities are up-to-date, clearly communicated, regularly rehearsed, implemented effectively, and readily available, in accordance with their significance, importance, or classification.

Managing the physical security controls of sites occupied by MoJ employees is the responsibility of a contracted provider. The physical security controls include, for example:

- Perimeter control.
- Guarding.
- Site access.

The controls are measured in the form of Physical Security Reviews, as undertaken by the Group Security and Governance Team.

It is the responsibility of those procuring supplier contracts for such physical security measures to ensure that the most up-to-date technical and industry standards are met, and that the technology and processes in place are regularly reviewed to ensure that the security controls remain effective and fit for purpose. This includes technical and industry standards for Closed Circuit Television, Access Controls, Intruder Detection Systems, and any other relevant alarm systems which are managed by a contracted supplier.

Policy statements

Physical Security controls **shall** be implemented that are proportionate to the risk appetite of the MoJ, and in adherence with the Information Security Policy and Acceptable Use Policy and other appropriate personnel and information security standards, including successful completion of the Baseline Personnel Security Standard.

All employees must ensure they remain observant, report any suspicious behaviour, and highlight non-compliance. This vigilance will help deter, delay, prevent, or detect unauthorised access to, or attack on, a location, and mitigate the impact should they occur.

Each MoJ occupied premises presents unique physical security challenges. The measures introduced to protect each site **shall** take into account the risk categorisation and the physical composition of that site. Effective approaches to Physical Security **shall** follow the **mandatory** Physical Security Standards.

The most senior grade manager, or SRO in "Moderate Risk" and larger locations, **shall** ensure that their site adheres to the Response Level Security Measures Policy, and ensure physical security risk assessment activity is conducted annually, and that the action plans created to address identified risks are implemented.

Compliance

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

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

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

Physical security advice

Physical security advice, including specific advice on this guidance, can be obtained by contacting MoJ Group Security: mojgroupsecurity@justice.gov.uk.

Media handling

Working securely with paper documents and files

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

Audience

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

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

POL.PPR.001: Agencies and arm's length bodies (ALBs) **shall** comply with this corporate framework but **can** establish their own arrangements tailored to operational needs and **should** supplement this framework with local policy or guidance for any business-specific risk.

Objective

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

Scope and Definition

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

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

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

Context

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

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

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

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

Responsibilities

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

Policy statements
Identifying the correct security level

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

POL.PPR.002: Within the **Official** classification, material does not normally need to have the classification written on it. However, particularly sensitive information **should** be marked with the **Official-Sensitive** handling caveat if it requires more robust access and handling controls to prevent more damaging consequences from disclosure.

POL.PPR.003: Information handled in the MoJ might not always have a visible classification marking. If any file contains material with a marking, then the cover of the file **should** be marked with the highest level of any of the contents.

To identify the right security level for information, think about:

- How sensitive that information is.

- Whether it contains personal data that could be used to identify individuals.
- What the consequences might be if the information was compromised or misused.
- Whether the information is likely to be under threat from anyone with a high intercept capability. If so, the information might require marking at a higher classification than **Official**. If you are working with information or documentation higher than the **Official** classification level, contact MoJ Group Security for specific guidance.

If you are in any doubt, ask your line manager or contact MoJ Group Security.

Allocating security levels and marking

POL.PPR.004: If you are generating original information, you **should** apply the standard rules to decide which classification to use. Do not set security levels higher than necessary. Set the classification that is appropriate at the time. Classification can be altered later if circumstances change, such as when material is no longer embargoed or has been released intentionally for consultation.

POL.PPR.005: For material at **Official-Sensitive** or higher classifications, the classification **shall** be written in capitals at the top and bottom of each page of the document. You **should** use the header and footer facility if creating electronically, and include page numbers by using the format `Page x of y`. You **should** only create documents at classification levels higher than **Official** on approved IT systems. If you are working with information or documentation higher than the **Official** classification level, contact MoJ Group Security for specific guidance. Files and documents **should** be marked according to the most sensitive piece of information included.

Data Protection Act

If the information in the documents or files can be used to identify living individuals, or could identify living individuals when used in conjunction with other MoJ material, then the information is covered by the Data Protection Act (DPA). The Act covers not only information such as name, address, and date of birth, but also expressions of opinion about or intentions towards an individual.

POL.PPR.006: Paper-based information that is covered by the DPA **should** be managed according to the general principles of working securely with paper documents and files set out here.

Handling paper-based information in the office

Think carefully before leaving papers unattended on desks, in the same way that you would avoid leaving your own personal correspondence – or even a purse or wallet – in plain view.

The MoJ has a clear desk policy that is intended to ensure information is seen only by people who 'need to know' it.

This means:

- Not leaving documents or files on a desk when not being used.
- Locking documents or files in a secure cabinet when you leave the office.

Failure to follow this policy could expose files and papers to the risk of being seen during the working day by other staff, or visitors to the office and, out of hours, by guards and cleaners. Even apparently non-sensitive information should be looked after. Putting papers away also protects them from damage from fire, smoke, or water.

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

Taking documents and files out of the office

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

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

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

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

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

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

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

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

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

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

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

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

Sending documents

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

Disposing of paper information

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

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

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

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

Long-term storage

The MoJ has arrangements for the secure long-term storage of paper documents and files. If you want to keep paper-based information, but no longer need to regular access to it, refer to the information on the MoJ Intranet regarding keeping, deleting, and disclosing information. The Records and Retention team can provide additional guidance.

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

POL.PPR.017: If you suspect that the security of the information you work with has been compromised in any way, you **shall** report it immediately.

Note: A security breach does not have to involve the actual loss of information. The potential loss of information also counts. For example, if a security cabinet has been left unsecured, there may be no evidence that any information has been lost or interfered with, but there is a clear potential for loss or damage.

Compliance

POL.PPR.018: The level of risk and potential impact to MoJ assets, and, most importantly, physical harm to our people and the public, determines the controls to be applied and the degree of assurance required. The MoJ **shall** ensure a baseline of physical security measures are in place at each site, and receive annual assurance that measures are in place to provide appropriate protection to all occupants and assets, and that these measures can be strengthened when required, such as in response to a security incident or change in the Government Response Level.

POL.PPR.019: The implementation of all security measures **shall** be able to provide evidence that the selection was been made in accordance with the appropriate information security standards ISO27001/27002, Physical Security advice taken from the Centre for the Protection of National Infrastructure (CPNI), and Government Functional Standard - GovS 007: Security.

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

Physical security advice

Physical security advice can be obtained by contacting MoJ Group Security.

Contact details

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

Glossary and Acronyms

Glossary

This information is a reference list of Ministry of Justice (MoJ) terms and abbreviations.

A more extensive list of acronyms is available here.

The NCSC has a comprehensive cybersecurity glossary available on its website.

Terms

2FA	Refer to Multi-factor authentication.
Authorised User	Any user of services covered as authorised by the MoJ.
Blue Team	The internal security defence team in an organisation. Within the MoJ, this work is performed by the Security Team.
Brute Force Attack	The application of lots of computer power, to try and perform a task using a huge number of values. Typically used to try out many passwords, to gain access to systems.
Business Continuity Plan (BCP)	A document that outlines the procedures in place for a business to continue to operate, despite an unexpected disruption to services. These disruptions might be things such as cyber attacks, pandemics, or natural disasters.
Credentials	Information used to prove someone's identity, to confirm that they really are who they say they are. Typically includes passwords, tokens, and certificates.

Critical infrastructure attack	Critical infrastructure refers to the physical and cyber structures, facilities, and systems that are essential for a country to function. Attacks on these resources would harm the physical security, economic security, or public health of the country.
Customer	Someone who buys goods or services. The customer of an IT service provider is the person or group who defines and agrees the service level targets. The term customers is also sometimes informally used to mean users, for example "this is a customer focused organisation".
Dark web	Generic name for encrypted online content that is not indexed by search engines. The information is only accessible with special software or tools.
Data breach	An incident where data is accessed in a non-authorised way.
Decryption	The reverse of an encryption process.
Distributed Denial of Service (DDoS) attack	Legitimate users cannot access computer services, because threat actors are overloading the service with requests. Also referred to as a Denial of Service (DoS) attack.
Digital footprint	A collection of data and information traces left behind by a user, as they do activities online. For example, all the things you've ever searched for on Google.
Double encryption ransomware	Refer to ransomware.
Encryption	The process of converting human-readable text into unreadable 'disguised' information, or 'ciphertext'. You can see it, but you can't understand it. Only someone with a decryption key can convert ('decrypt') the unreadable information back into human-readable form again.
Exfiltrate	The formal name for a technique used by threat actors and malware to surreptitiously copy and transfer data out of a system. This is data theft.
Exploit	A program or process that takes advantage of a vulnerability in a system to cause system problems, or to access or modify information without authorisation.
Incident	Any event which is not part of the standard operation of a service, and which causes, or might cause, an interruption to, or a reduction in, the quality of that service. A breach of the security rules for a system or service.
Incident Management	The process responsible for managing the lifecycle of all incidents. The primary objective of incident management is to return the IT service to users as quickly as possible.
Insider threat	Any threat from current or former employees of an organisation who have inside information or authorised credentials that might be used to cause harm to the organisation, accidentally or maliciously.

Macro	A small program or script that automates tasks in an application, such as Microsoft Office. Might be used by attackers can use to gain access to, or harm, a system.
Malware	Malicious software. This includes things like viruses, trojans, worms, or any code that can have a negative impact on an a system.
Multi-factor authentication (MFA)	Use of two or more different components to verify a user's claimed identity. Typically an extra component, in addition to a password. MFA often uses an authenticator app or SMS text to deliver a single use code. Also Two-factor authentication (2FA).
Open Source Intelligence (OSINT)	Information gathered from public information. This includes data from social network accounts, company websites, and other openly available information sources.
Operational Security Team (OST)	Deprecated name for the Security Team within the MoJ. The Security Team help protect against cyber attacks, and help manage incidents. Sometimes referred to as the Blue Team. They can be contacted through email: security@justice.gov.uk.
Out of band check	An additional check performed using a different communication channel, to verify identity or intent. The check helps prevent phishing or social engineering attacks. For example, if you receive an email from a senior manager, asking you to perform an unusual task, you should want to check that the request is genuine. If you reply by email to the original request, that's an 'in band' check, and can't be trusted, because it's possible the manager's email has been compromised. But if you called the manager by mobile phone to check the request, that's using a different communication technology, so it's an out of band check. A threat actor would have to compromise both the manager's email and their mobile phone account to succeed in tricking you. For more detail on out of band checks, refer to this additional information.
Password	A secret string of characters, numbers, and often symbols. When used with a valid user ID, a password enables access to an account.
Patching	Applying updates to software or firmware to improve security and enhance functionality.
Phishing	Untargeted mass emails sent to many individuals. The email typically asks for sensitive information, or encourages you to visit fake websites, or to send money. For more information, refer to the phishing guide.
Problem	A cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the Problem Management process is responsible for further investigation.
Problem Management	The process responsible for managing the lifecycle of all problems. The primary objectives of Problem Management are to prevent incidents from happening,

	and to minimise the impact of incidents which cannot be prevented.
Process	A structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. A process might include any of the roles, responsibilities, tools, and management controls required to deliver the outputs reliably. A process might define policies, standards, guidelines, activities, and work instructions if they are needed.
Ransomware	Malicious software that makes data or systems unusable by encrypting it and then demanding a payment from the victim to decrypt it. Double Extortion Ransomware exfiltrates the data before encryption and demands a ransom payment to stop the threat actor releasing the data to the public, as well as for decrypting the system.
Red team	This is an internal or external team that tests organisational security by simulating cyber attacks as realistically as possible. Together with the Blue Team, the team helps to improve the cyber defences of the organisation.
Resolution	Action taken to repair the fundamental cause of an incident or problem, or to implement a workaround.
Resolver Group	May include a wide range of IT teams, including support and development personnel, other Service Management Functions (SMFs), other units within the organisation, outsourcing providers, partners, and other third parties.
Service Desk	The single point of contact between the service provider and the users. A typical Service Desk manages incidents and service requests, and handles communication with the users.
Social engineering	Manipulating people into doing things or divulging information that is of use to a threat actor.
Tabletop	An exercise created to try out Business Continuity Plans (BCPs). These exercises create realistic scenarios, and play through a number of obstacles, to ensure organisations have robust BCPs.
Tailgating	An unauthorised individual forcefully or stealthily gaining access to a building, typically by entering immediately behind an authorised user.
Threat actor	A general term that encompasses all types of individuals and groups that use cyber methods to cause harm. This includes competitors seeking to steal information, cyber criminals attacking for political or monetary gain, accidental or malicious insider threats, spies, social and political activists, and assorted hackers.
Trend Analysis	Analysis of data to identify time related patterns. Trend analysis is used in Problem Management to identify common failures or fragile configuration items, and in Capacity Management as a modelling tool to predict future behaviour. It is also used as a management tool

	for identifying deficiencies in IT Service Management Processes.
Virtual Private Network (VPN)	An encrypted network created to allow secure connections for remote users.
Vulnerability	A weakness in software, a system, or process. A threat actor might seek to exploit a vulnerability to gain unauthorised access to a system.
Zero day (0day)	A vulnerability in a system that few people know about. threat actors can exploit an 0day to attack or affect data and systems.
Zero trust	The assumption that all requests and connections are potential breaches, and so must be verified and authenticated before being allowed.

Out of band checks

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

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

Example 1: You receive an email request for an urgent review of an invoice, and immediate payment. The email comes from someone unexpected. You should find the official contact details of that person, and contact them using a phone call - but not email - to confirm that they did indeed send the original email. If they did send the email, you can proceed with the request. If they did not send the email, you can report the email as a phish, and also alert the owner of the email address that their email address might have been compromised.

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

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

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

When doing an out of band check, be sure to pick a different method of communication to the one used to contact you originally. If someone emails you unexpectedly, perform an out of band check by making a phone call. If someone

calls you, perform an out of band check by using the Internet. It is very unlikely that multiple communication channels have been compromised.

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

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

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

Contact details

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