# Ministry of Justice (MoJ)
# Cyber Security Guidance

# Contents

# Cyber and Technical Security Guidance

## Summary

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

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

**Note:**

This guidance is dated: 16 November 2020.

This offline version of the guidance is available as a PDF file for convenience. However, it is time-limited: it is not valid after 16 December 2020. For the latest, current version of the guidance, see here.

### Getting in touch

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

## Information structure

The documents are listed in the next section.

Content tagged with the Intranet icon (  ) is on the MoJ Intranet. You will need Intranet access to view that content.

### Information security policies

#### Management direction for information security

| | |
|---|---|
| Avoiding too much security | All users |
| IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER | All users |
| Line Manager approval | All users |

### Mobile devices and teleworking

#### Mobile device policy

| | |
|---|---|
| Remote Working | All users |

#### Teleworking

| | |
|---|---|
| Accessing MoJ IT Systems From Abroad | All users |
| General advice on taking equipment abroad | All users |
| Security Guidance for Using a Personal Device | All users |

## Human resource security

### Prior to employment

| | |
|---|---|
| Personnel security clearances | All users |

### During employment

| | |
|---|---|
| Training and Education | All users |

## Asset management

### Responsibility for assets

| | |
|---|---|
| Acceptable use | All users |
| Acceptable use policy | All users |
| IT Acceptable Use Policy | All users |
|  Protect Yourself Online | All users |
|  Web browsing security | All users |

### Information classification

| | |
|---|---|
|  Government Classification Scheme | All users |
| `OFFICIAL` and `OFFICIAL-SENSITIVE` | All users |

### Media handling

| | |
|---|---|
|  Removable media | All users |
|  Secure disposal of ICT equipment | All users |

## Access control

### User access management

| | |
|---|---|
| Minimum User Clearance Levels Guide | All users |

### User responsibilities

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

### System and application access control

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

## Physical and environmental security

### Equipment

| | |
|---|---|
|  Clear Screen and Desk Policy | All users |
|  Laptops | All users |
|  Locking and shutdown | All users |
|  Policies for Macbook Users | All users |

## Operations security

### Control of operational software

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

## Communications security

### Information transfer

| | |
|---|---|
| Bluetooth | All users |
| Email security | All users |
| General Apps Guidance | All users |

## Information security incident management

### Management of information security incidents and improvements

| | |
|---|---|
|  Forensic Principles | All users |
| Lost Laptop or other IT security incident | All users |
| Reporting an incident | All users |

## Compliance

### Compliance with legal and contractual requirements

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

## Risk Assessment

### Risk Assessment Process

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

## Other Guidance

### Intranet

There are other cyber and technical security guidance documents available to reference. A large number of these documents are available in the IT and Computer Security repository on the MoJ Intranet, but these documents are currently being reviewed and progressively are being incorporated into this main Security Guidance repository.

### Technical Guidance

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

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

# Getting in contact

## Reporting an incident

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

Suppliers to the MoJ should refer to provided methods/documentation and contact your usual MoJ points of contact.

## Cyber Security Consultancy Team: asking for help

### Overview

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

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

### About the team

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

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

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

### Asking for help

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

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

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

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

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

### How the Consultancy team handle requests for help

Each working day, we review all new requests.

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

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

### What happens next

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

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

### If things go wrong...

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

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

# Information security policies

## Management direction for information security

### Avoiding too much security

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

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

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

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

An example is a domain name or IP address. These values do not need to be secret for all systems. Only those that need it. It might be tempting to say that 'all IP addresses are `OFFICIAL-SENSITIVE`. This is then used as a reason for an (in)action, such as "I can't email you that network diagram because it contains IP addresses." But the statement

has wider consequences. It imposes a set of security requirements for everyone. It imposes them irrespective of the actual secrecy required.

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

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

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

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

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

### It's not only about domain names or IP addresses

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

## IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

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

### The Standard

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

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

#### IDENTIFY

IDENTIFY is a prerequisite standard that requires:

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

#### PROTECT

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

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

#### DETECT

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

- capture event information (and apply common threat intelligence sources, such as CiSP);

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

### RESPOND

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

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

### RECOVER

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

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

## Line Manager approval

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

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

- General advice on taking equipment abroad.
- Security Guidance for Using a Personal Device.

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

### Steps to follow (Line Managers)

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

1. Check that your direct report (DR) has said what they want in their request. The request should identify which MoJ IT Policies apply.
2. Check that the request is valid from a business perspective. If not, deny the request (step 7 ).
3. Check that Acceptable Use is in the list of applicable policies.
4. Review the requirements or obligations within the MoJ IT Policies that apply to the request.
5. Check that the DR understands and will follow the requirements or obligations. For example, have a discussion with them, or ask them for more information or evidence.
6. If they are able to follow the applicable MoJ IT Policies, send a formal approval to the DR. An email is enough for this.
7. If you don't think they can follow the Policies, or there's a weak business case for the request, refuse it.
8. Keep a copy of your formal reply, in accord with Data Retention requirements.
9. Some MoJ IT Policies need a copy of formal approval for other parties. For example, before your DR travels to some countries on MoJ business, send a copy of your approval to Operational Security: OperationalSecurityTeam@justice.gov.uk.

#### Steps to follow (Direct Reports)

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

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

# Mobile devices and teleworking

## Mobile device policy

### Remote Working

#### Key points

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

#### Overview

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

#### Audience

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

### What is remote working?

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

### Protecting your workspace and equipment

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

**Always:**

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

**Never:**

- Let family or other unauthorised people use MoJ equipment.
- Leave equipment unattended.
- Work on sensitive information in public spaces, or where your equipment can be overlooked by others.
- Advertise the fact that you work with MoJ materials.
- Take part in conference or video calls when you are in public or shared spaces such as cafes or waiting rooms.
- Send work material to your personal email address.

### Working securely

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

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

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

### Using your own equipment

The main guidance is available here.

Wherever possible, you should always use official MoJ equipment for business purposes. Never send work material to your personal email accounts.

If you are working remotely, or do not have access to MoJ equipment, it might be tempting to use your own equipment, especially printers. The advice is to avoid printing anything, and in particular not to use personal printers.

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

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

Basically, think before you print.

### Privacy

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

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

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

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

### Contacts for getting help

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

### General enquiries, including theft and loss

**Dom1/Quantum - Technology Service Desk**

- Tel: 0800 917 5148

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

**Digital & Technology - Digital Service Desk**

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

**HMPPS Information & security:**

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

### Incidents

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

**Operational Security Team**

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

### Privacy Advice

**Privacy Team**

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

### Cyber Security Advice

**Cyber Consultants & Risk Advisors**

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

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

**MoJ HQ staff**

- Email: Records_Retention_@justice.gov.uk

**HMCTS and HMPPS staff**

- Email: BranstonRegistryRequests2@justice.gov.uk

### JustStore

- Email: KIM@justice.gov.uk

### Related information

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

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

HMPPS Advice

Last updated: April 24th, 2020.

# Teleworking

## Accessing Ministry of Justice (MoJ) IT Systems From Abroad

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

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

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

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

- Do you need to take MoJ IT equipment abroad or access MoJ IT systems to do your job?
- Can the business need be met in another way or by someone else?
- If you just need to manage your inbox while away, can you delegate permissions to your inbox to a colleague to manage on your behalf?
- Have you left enough time to check and obtain necessary approvals? The process can take several weeks, depending on the circumstances. This is because it may be necessary to apply additional technical controls to protect you, your device, and any data the device can access.

### Steps to follow before travelling
### Part One

1. Get confirmation from your Line Manager that there is a business need for you to take MoJ equipment abroad and access MoJ services. Keep a note of the answers you get.
2. Proceed directly to Part Two of this process if *either one* of the following two statements apply to you:
    - You are travelling or passing through one of the following high-attention countries: *China, Cyprus, Egypt, France, Germany, India, Iran, Israel, North Korea, Pakistan, Russia, Saudi Arabia, South Africa, South Korea, Syria, Turkey, UAE*.
    - You are national security cleared to 'Enhanced SC' or DV levels.
3. If you have reached this step, you do not need to seek further formal approval for your trip.
4. Take a copy of this guidance; it includes useful contact details that help in the event of a problem while travelling.
5. Check if you need to do anything to prepare for International Roaming.

6. Enjoy your trip.

### 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.
    - The make/type of equipment you want to take with you.
    - Asset Tag details.
    - Countries you'll be visiting or passing through.
    - Dates of travel.
    - Transport details where possible, for example flights or rail journeys.
    - Proposed method of connecting, for example MoJ VPN.
    - Reason for maintaining access while abroad.
    - The MoJ data, applications, or services you expect to access during your trip.
    - Who you are travelling with.
2. The next step depends your MoJ business area:
    - If you are part of MoJ HQ, HMPPS HQ or HMCTS, contact your Senior Civil Servant (SCS) and ask for approval to take MoJ equipment abroad 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 abroad 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 request form.
4. Send the completed form to security@digital.justice.gov.uk, including the answers obtained from the earlier parts of this process.
5. Your request is considered, and an answer provided, as quickly as possible.
6. When you have received all the approvals, send a copy of your request and the approvals to OperationalSecurityTeam@justice.gov.uk.
7. When Operational Security have acknowledged receipt of the request and approvals, the formal process is complete.
8. Check if you need to do anything to prepare for International Roaming .
9. Take a copy of this guidance; it includes useful contact details that help in the event of a problem while travelling.
10. Enjoy your trip.

### International Roaming

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

By default, MoJ equipment is not enabled for use abroad. Before travelling, contact the MoJ Phone and Mobile Devices team. Ask them to enable International Roaming, and to activate the remote wipe function. This helps protect the MoJ equipment in case of loss or theft.

### If you have any problem when using MoJ equipment abroad

Contact the 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 Corporate Security Branch as soon as possible.

For any emergency outside normal UK business hours, contact the Duty Security Officer.

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

### Related pages

- General advice on taking Equipment abroad
- Overseas travel
- Staff security and responsibilities – during employment

### External websites

- Foreign & Commonwealth Office – travel & living abroad

### Contacts

### Operational Security Team

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

### Dom1 - Technology Service Desk

- Tel: 0800 917 5148

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

### Digital & Technology - Digital Service Desk

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

### MoJ Duty Security Officer

- Tel: +44 (0)20 3334 5577
- Email: dutysecurityofficer@justice.gov.uk

### MoJ Phone and Mobile Devices

- Email: MoJ_Phone_and_Mobi@justice.gov.uk

### MoJ Security

- Email: security@Justice.gov.uk

## General advice on taking equipment abroad

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 abroad 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 abroad so that the risk of data exposure is reduced in case of loss or theft.

### Keeping safe whilst conducting sensitive work abroad

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

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

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

### Guidance on using mobile phones

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

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

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

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

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

If you are on official business:

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

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

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

### Contacts 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

**Dom1/Quantum - Technology Service Desk**

- Tel: 0800 917 5148

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

**Digital & Technology - Digital Service Desk**

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

**HMPPS Information & security:**

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

### Incidents

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

**Operational Security Team**

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

## Security Guidance for Using a Personal Device

### Summary

Not everyone has access to an Ministry of Justice (MoJ) device which can be used remotely. In these extraordinary times, exceptional provision is being developed for you to use your own devices for work purposes.

Until that provision is in place, you must not use a personal device for work purposes.

### Guidance

- If you have an MoJ-issued device, you must use that.
- You may not use Office 365 tools (email, calendar, Word, Excel, Powerpoint, etc.) for work purposes on a personal device (desktop, laptop, tablet or phone). This applies to web browser and installed client applications.
- Do not send MoJ information to your personal email account, or use personal accounts for work purposes.
- Do not store work files or information on a personal device (desktop, laptop, tablet or phone).
- Some teams within the MoJ, such as groups within Digital & Technology, and HMCTS, might already have prior permission to use personal devices for aspects of software and service development work. This permission continues, but is being reviewed on an on-going basis.

This guidance applies to all staff and contractors who work for the MoJ. It provides advice about using your personal devices for work purposes.

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

Last updated: April 24th, 2020.

# Human resource security

## Prior to employment

### Personnel security clearances

#### Baseline Personnel Security Standard (BPSS)

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

The BPSS is published on GOV.UK.

#### National Security Clearances

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

## During employment

### Training and Education

#### Why?

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

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

#### Source

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

# Asset management

## Responsibility for assets

### Acceptable use of Information Technology at work

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

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

### Summary

Be sensible when using MoJ IT resources:

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

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

### What is meant by IT?

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

### Acceptable use of MOJ IT

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

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

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

### Unacceptable use of MoJ IT

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

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

- Deliberately or accidentally sharing resources or information, such as passwords, with people who are not supposed to have them.
- Using resources without permission.
- Storing sensitive information where it could easily be lost or stolen.
- Using your work email address for personal tasks.
- Using a personal account or personal email address for work tasks.
- Excessive private use during working time.
- Installing unlicensed or unauthorised software.

### Why unacceptable use is a problem

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

- Bad publicity or embarrassment.
- Increased or unexpected costs or delays.
- Civil or legal action.

- Reduced efficiency and effectiveness.

Unacceptable use might also affect you, too:

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

### Keeping control

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

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

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

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

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

### Personal use of MoJ IT

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

### Personal use of MoJ mobile phones

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

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

This usage must always be for work purposes.

Examples of unacceptable MoJ mobile phone use include:

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

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

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

### Using MoJ IT outside your usual workplace

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

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

### Avoid using removable media

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

### Personalisation of equipment

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

## Acceptable use policy

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

Guidance about Acceptable Use of IT within the MoJ is available here.

The definitive list of Acceptable Use Policy statements is available here.

## IT Acceptable Use Policy

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

### Introduction

MoJ ICT systems and services are first and foremost provided to support the delivery of MoJ's business services. To achieve this, most MoJ users are provided with an appropriate general purpose computer environment (i.e. a standard MS Windows desktop) and access to services and communication tools such as e-mail and the Internet.

This policy outlines the acceptable use of MoJ IT systems and services, and, expectations the MoJ has on its staff in this area.

### Scope

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

Failure to adhere to this policy could result in:

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

| | |
|---|---|
| **POL.ITAUP.001** | All Users **must be** made aware of the IT Acceptable Use Policy (this document) and provided with security awareness training which covers this policy. |
| **POL.ITAUP.002** | All Users **must undergo** refresher security awareness training which covers this policy every 12 months. |

### Protection of assets

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

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

It is important that all Users of an ICT system (include support and system administrative Users) are familiar with these SyOPs and are provided with the appropriate training.

| | |
|---|---|
| **POL.ITAUP.003** | All ICT systems **must have and maintain** a set of Security Operating Procedures (SyOPs). For systems undergoing the Accreditation process, these SyOPs can be included as part of the RMADS. |
| **POL.ITAUP.004** | All Users of an ICT system (this includes support and system administrative staff) must read the SyOPs applicable and **must acknowledge** that they have both read and understood it before being granted access. A record must be kept of this event and made available to the system Accreditor upon request. |
| **POL.ITAUP.005** | All Users **must be** made aware that non-conformance to system SyOPs constitutes a breach of the MoJ IT Security Policy which may result in disciplinary action. |
| **POL.ITAUP.006** | Any change to an ICT system's SyOPs **must be** approved by the system Accreditor in advance. |
| **POL.ITAUP.007** | Any request to perform an action on an ICT system which contravenes its SyOPs **must be** approved by the system Accreditor or MoJ ITSO in advance. |

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

### General Security Operating Procedures (SyOPs)

The policy refers to a key set of general SyOPs which are listed below:

- IT Security Operating Procedures - System Administrators.
- IT Security Operating Procedures - Administrators and Users.
- Remote Working.
- IT Security Operating Procedures - ICT Equipment: Desktop – Corporate.
- IT Security Operating Procedures - ICT Equipment: Mobile Devices - RAS Laptop.
- IT Security Operating Procedures - ICT Equipment: Mobile Devices – Blackberry.

To minimise the number of SyOPs in circulation and standardise procedures, the SyOPs listed above act as the primary set where individual ICT systems are expected to conform to in terms of their own SyOPs. Any deviations or additions are at the discretion of the system Accreditor.

| | |
|---|---|
| **POL.ITAUP.008** | All ICT systems **must have** documented SyOPs which comply with the general SyOPs listed in this policy (see here ). Any deviations or additions must be recorded in separate SyOPs which form an addendum to one of the SyOPs listed here. |

**Note** – An ICT system may make use of, in their entirety, one or more of the SyOPs listed above as the procedures of that IT system do not deviate from those described in these general SyOPs.

### Removable Media

Removable storage media include devices such as USB memory sticks, writeable CDs/DVDs, floppy discs and external hard drives. These devices can potential contain large amounts of protectively marked data and pose a significant risk to the Confidentiality of data held on them. As such, the MoJ controls the use of removable media through SyOPs, technical security controls, and requiring movements of bulk data to be authorised by MoJ ICT IA, this includes completing an Information Asset Movement Form.

| | |
|---|---|
| **POL.ITAUP.009** | Any removable media device **must be** approved by MoJ ICT IA where that device is used to store protectively marked data. The type of device and associated SyOPs must be approved by the system Accreditor prior to operational use. |
| **POL.ITAUP.010** | All Users **must ensure** that all data stored on or transported by removable media is in accordance with the applicable system SyOPs. |
| **POL.ITAUP.011** | All Users **must seek** approval from MoJ OST prior to any bulk transfer of protectively marked data using removable media. MoJ ICT IA will advise on any technical and procedural requirements such as data encryption and handling arrangements. |

### Passwords

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

| | |
|---|---|
| **POL.ITAUP.012** | All Users **must not** share or disclose any passwords with any other person. |
| **POL.ITAUP.013** | All Users **must not:**<br>• Attempt to gain unauthorised access to another User's IT account.<br>• Attempt to use another Users access credentials to gain access to an ICT system.<br>• Attempt to access information for which they do not have a 'need-to-know'.<br>• Use the same password on more than one ICT system. |

### Legal and regulatory requirements

There are a number of legal and regulatory requirements for which the MoJ must comply with, this in addition to HMG security policy as expressed in the HMG Security Policy Framework.

| | |
|---|---|
| **POL.ITAUP.014** | All Users **must be** made aware of legal and regulatory requirements they must adhere to when accessing MoJ ICT systems. This must be included as part of the SyOPs. |

### MoJ's Corporate Image

Communications sent from MoJ ICT systems or products developed using them (e.g. MoJ branded document or PowerPoint presentation) can damage the public image of the MoJ if, it is for purposes not in the interest of the MoJ, or, it is abusive, offensive, defamatory, obscene, or indecent, or, of such a nature as to bring the MoJ or any its employees into disrepute.

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

### Potential to cause offence and harm

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

| | |
|---|---|
| **POL.ITAUP.016** | MoJ ICT systems **must not** be used for any activity that will cause offence to MoJ employees, customers, suppliers, partners or visitors, or in a way that violates the MoJ Code of Conduct. |

### Personal use

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

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

- Filtering of Internet and e-mail traffic – All Internet and e-mail traffic is filtered and analysed, further details are provided here.
- Policy and procedures – This policy and associated SyOPs set out the restrictions placed on the use of an ICT system.

| | |
|---|---|
| **POL.ITAUP.017** | Users **must ensure** any personal use of MoJ ICT systems does not conflict or interfere with normal business activities. Any conflict is to be reported to their line manager. |
| **POL.ITAUP.018** | Users **must ensure** that any personal use of MoJ ICT systems is inline with any applicable SyOPs and this policy. |
| **POL.ITAUP.019** | Users **must be** aware that any personal use of MoJ ICT systems which contravenes any applicable SyOPs, or this policy, constitutes a breach of the IT Security Policy and may result in disciplinary action. |

### Maintaining system and data integrity

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

| | |
|---|---|
| **POL.ITAUP.020** | All Users **must request** any changes to ICT system/s or ICT equipment through the IT helpdesk. Further details are provided in IT Security Operating Procedures - Administrators and Users. |

### Electronic messaging and use of the Internet

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

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

Also, the use of any high bandwidth services, such as video steaming websites, creates network capacity issues which cause the poor performance key MoJ ICT services. As such, the MoJ restricts access to the Internet based on job role. Amendments can be made on the submissions of a business case for approval by MoJ Operational Security Team (OST).

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

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

| | |
|---|---|
| **POL.ITAUP.021** | All Users **must use** the Internet and e-mail (and other electronic communication systems) in accordance with this policy document. |

### Managing e-mail use

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

The MoJ is connected to the Government Secure Intranet (GSi), which provides a secure environment for sending/receiving E-mails between Government departments. This allows Users with a MoJ E-mail account (e.g. suffix '`@justice.gsi.gov.uk`') to send E-mails which attracts a protective marking up to and including `RESTRICTED` to another MoJ or government User where their E-mail suffix ends in '`.gsi.gov.uk`'.

| | |
|---|---|
| **POL.ITAUP.022** | All Users **must ensure** that protectively marked information contained within or attached to an e-mail is handled in accordance with ICT Security - Information Classification and Handling Policy. |

E-mail is a major source of malware and route into the MoJ for criminal organisations to defraud staff or exfiltrate information. All Users need to exercise care when handling emails and report any suspicious activity as an IT security incident.

| | |
|---|---|
| **POL.ITAUP.023** | All Users **must ensure** that they do not:<br>• Open any attachments to an E-mail where the source is untrusted, unknown or unsolicited.<br>• Click on any links within an E-mail where the source is untrusted, unknown or unsolicited. |
| **POL.ITAUP.024** | Where a User suspects that an E-mail received is from an untrusted, unknown or unsolicited source, they **must** report it as an IT security incident. |

### Connectivity and remote access

Remote access is provided to MoJ ICT systems and services allowing Users access from offsite and home locations to connect in. The main methods of access are either via a RAS laptop and/or Blackberry device. In the main, remote access is to a protectively marked MoJ IT system (up to and including `RESTRICTED`). As such Users need to be aware of both the security controls and procedures of the device used as well as the general physical security considerations. This includes any restriction on the carriage of such devices as they may contain HMG protectively marked data and HMG cryptographic material.

MoJ ICT IA maintains a list of countries where carriage and use of remote access devices is permitted. Further details can be found in the Remote Working guidance.

| | |
|---|---|
| **POL.ITAUP.025** | All Users **must be** aware of the Remote Working guidance and must confirm that they have read and understood it before being provision with any remote access devices or equipment (e.g. RSA token). |

| | |
|---|---|
| **POL.ITAUP.026** | Any User wishing to take a remote access device out of the UK **must consult** Remote Working before doing so or the applicable device IT Security Operating Procedures document. |

### Monitoring of communications

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

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

The MoJ, so far as possible and appropriate, respects the privacy and autonomy whilst working of all Users, but further to this information, any personal use of MoJ ICT systems will also be subject to monitoring. By carrying out personal activities using MoJ ICT systems, Users are consenting to the MoJ processing any sensitive personal data which may be revealed by such monitoring (for example regular visits to a set of websites).

For the purposes of business continuity it may sometimes be necessary for the MoJ to access business communications (including within e-mail mailboxes) while a User is absent from work (including holiday and illness). Access will only be granted through submission of a formal request to the IT Helpdesk where approval is required from the relevant line manager where the MoJ ITSO and MoJ HR may be consulted.

| | |
|---|---|
| **POL.ITAUP.027** | All Users **must be** aware their electronic communications are being monitored in accordance with this policy. |
| **POL.ITAUP.028** | All Users **must be** aware that business communication (such as e-mail mailboxes) may be accessed if they are absent from work. This can only be requested and authorised by a line manager where the MoJ ITSO and MoJ HR may be consulted. |

# Information classification

## OFFICIAL, OFFICIAL-SENSITIVE

h/t https://www.gov.uk/guidance/official-sensitive-data-and-it

### OFFICIAL

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

### OFFICIAL-SENSITIVE

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

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

### DESCRIPTORS

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

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

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

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

Descriptors are **not** codewords.

# Access control

## User access management

### Minimum User Clearance Requirements Guide

#### Introduction

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

#### Security clearance levels

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

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

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

#### Minimum user clearance requirements

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

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

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

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

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

Please contact the Cyber Assistance Team and refer to the Vetting Policy for further information.

### Checking someone's clearance status

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

- Their firstname.
- Their lastname.
- Their date of birth.

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

### Contact details

Contact the Cyber Assistance Team for advice - CyberConsultancy@digital.justice.gov.uk

# User responsibilities

## Protecting Social Media Accounts

### Summary

Hostile attacks on Social Media accounts pose a serious threat to the Ministry of Justice (MoJ) and its reputation. When attacks happen, they quickly become headline news, and can happen to any account, anywhere in the world.

Two types of attacks are common:

- Attempts to render the account useless by 'bombarding' it with messages.
- Attempts to 'take over' the account.

### Steps we can all take to protect ourselves
### Ensure our passwords are secure

Passwords are the main protection on our accounts, hence ensuring they are secure is vital. The NCSC has produced guidance on making secure passwords - the summary of which is that picking three random words to make a password (for example `RainingWalrusTeacup`) is a good policy for securing Social Media accounts.

### Check your email details are up-to-date

Most of the time, the first indication you'll have that something is wrong is when an email is sent to you. This could be to let you know that someone is attempting to log into your account, or that someone is trying to reset your password, or more worringly, that a new device has logged into your account. Hence it is important that you ensure that your email details are up-to-date, and that your email is secure.

### Enable Two Factor Authentication

Two Factor Authentication (2FA) involves requiring a random code to be entered before being logged in. These codes are either sent to the user via SMS or email, or generated every 30 seconds by an app or device the user has which relies on a seed key provided by the service. That seed can then be shared amongst a team, allowing for multiple owners or contributors.

If at all possible, SMS generation should be avoided, as it is theoretically possible for phone numbers to be taken over through various attacks, as well as meaning that only one person can receive the code, which isn't ideal if a team is working on a single account.

If you're using email, then it can be sent to a group account, which also allows for multiple owners or contributors - but it's important to ensure that the email is also protected by 2FA.

If you have a spare 10 minutes, watch this video for an excellent explanation of how 2FA works and why it's important to have it enabled.

Click the links for details on how to activate 2FA for Facebook, Twitter and Instagram.

### Only use trusted third-party applications

In addition to the official applications, there are many tools and third-party applications that might be used to work with social media accounts.

Some of these tools provide useful extra facilities, such as 'scheduled' posts, or helping you post one message to several different social media channels.

The problem is that you have to give your account details to these tools so that they can post to your account.

This is potentially very dangerous:

- An application might post messages on your behalf, that you do not agree with or are unacceptable.
- An application might store or share your account details.

Only use applications that are trusted and approved for use with your social media accounts. For help with this, contact Cyber Security.

### Remove 'unused' applications

People tend not to be very good at removing old or rarely used applications. Older applications should be checked regularly to see if there are any updates.

A good habit is to check your applications once a month or so, and consider:

- Do you still use the application? If not, remove it.
- Whether there is an update available for the application? If so, install it.

As well as increasing safety, removing unused applications frees up storage space on your system.

### Check your privacy settings

The whole point of a social media account is to share information. But that doesn't mean you want to share *everything*.

When you first create a social media account, you are normally asked to decide on the privacy settings. These control how much information you share, and who you share it with.

But it's very easy to forget to check the settings, from time-to-time, to make sure they are still correct.

A good habit is to check your account privacy settings once a month or so. Information on privacy settings is available for the main social media environments:

- Facebook
- Twitter
- Instagram

### Limit access to your accounts

You might be tempted to share access to your social media account, for example if you want to have postings regularly, even while you are away.

Avoid sharing access to your social media account. It's easy to forget who the details are shared with. It's also possible that postings might be made on your behalf that you don't agree with, or are not acceptable.

Any MoJ social media accounts that do need to be shared will have proper access controls in place. You should never need to share your account details for work purposes.

If you need more help on this, contact your Line Manager or Cyber Security.

### Don't click on suspicious links

Unfortunately, social media postings are a common way of sending you links to malware or other problem material. Postings might also be used to send you 'phishing' attacks.

In the same way that you should be careful with any links or attachments sent to you using email, you should also be suspicious of links or attachments sent to you though social media. This applies to both general postings and messages sent directly to you ('Direct Messages').

For more information, read this article on the MoJ Intranet.

#### What to do if your account is bombarded
#### Remember that these attacks are short lived

Due to the amount of organisation and effort required to coordinate such an attack, they do not last long, and like an intense inferno, will soon burn themselves out.

#### Do not respond to the attack

These attacks are designed to attack the person controlling the account as well as the agency itself. By only responding to messages not involved in the attack - especially those trying to share positive messages, the attackers will run out of interest far sooner than if you engage them. If they are posting harmful or threatening messages, report the accounts.

In a single sentence - "don't feed the trolls".

#### Feel free to walk away

Dealing with these attacks can be emotionally draining; even just reading the messages can have a far greater impact on you than you realise. Take breaks in the event of an attack, even if it's hard to - consider going for a walk to force yourself away.

#### Cyber Security Advice

**Cyber Consultants & Risk Advisors**

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

# System and application access control

## Password Managers

### Overview

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

But how do you remember all these different passwords?

The simplest way is to use a Password Manager. If you have lots of different, and complex, passwords for all your accounts, using a password manager makes life much easier.

This article provides guidance on using password managers within the MoJ.

### What is a password manager/vault?

A password manager stores sensitive information in an encrypted form. Password managers are sometimes called password vaults.

In the MoJ, 'password managers' are tools that you might use for your personal accounts. 'Password vaults' are tools that a team of people might use to look after details for shared accounts.

Password vaults usually have extra strong access controls, such as hardware tokens.

Here, we use 'password manager' and 'password vault' interchangeably, except when stated otherwise.

### When do you use a password manager or a password vault?

The following table shows when you might use a password manager or vault:

| Scenario | Tool | Notes |
|---|---|---|
| Single user, personal accounts | Password manager | For accounts that only you use, or have access to, then you would probably store the details in a password manager. An example would be storing the username and password for your work email account; only you should have access. |
| Multiple users, shared accounts | Password manager or password vault | Some accounts might be shared between a group of users. For example, a team might need to know the password for an encrypted document. If the access required is for a sensitive or operational system, then a more heavily protected tool such as a password vault might be appropriate. |
| System access, no human use | Password vault | Some MoJ systems need to 'talk' directly to other systems. No humans are involved in the conversation. The passwords protecting these communications can - and should - be extremely complex. A strongly secured password vault would be ideal for this purpose. |

### Best practices

The NCSC is very clear:

> "Should I use a password manager? Yes. Password managers are a good thing."

This is helpful for us in the MoJ, as much of our IT Policy and guidance derives from NCSC best practices.

### What makes a good password manager?

A password manager should never store passwords in an unencrypted form. This means that keeping a list of passwords in a simple text file using Notepad would be A Bad Thing.

Good password managers encrypt the passwords in a file using strong encryption. It shouldn't matter where you store the encrypted file. Storing the list 'in the cloud' lets your password manager access the data from any device. This is useful if you are logging in from a laptop, or a mobile device. Storing the passwords locally means the password manager works even when offline.

A good password manager will have:

- Strong encryption for the list of passwords.
- Network access for encrypted lists stored 'in the cloud'.
- A dedicated app but also a 'pure' web browser method for working with your password list.
- A tool to generate passwords of varying complexity.
- The ability to fill in login pages.

### What password manager should I use?

In the NCSC article, they are very careful not to identify or recommend a password manager. This ... caution ... is the reason why we don't say much about password managers within the MoJ guidance.

There are several password managers used within the MoJ. LastPass and 1Password are probably the most popular for personal or team passwords. Example password vaults would be Hashicorp Vault, Kubernetes Secrets or AWS Key Management.

For individual use, have a look at LastPass and 1Password. See which one you like best, and try it out. When you decide on a password manager, request approval from your line manager to install and use it: "I'm planning to install and use XYZ to manage my passwords, is that OK?".

See also Using LastPass Enterprise.

# Passwords

## Overview

This article provides guidance on passwords within the Ministry of Justice (MoJ). It helps you protect MoJ IT systems by telling you about choosing and using passwords. Whenever you see the word 'system' here, it applies to:

- Hardware, such as laptops, PCs, servers, mobile devices, and any IT equipment.
- Software, such as the Operating System, or applications installed on hardware, or mobile device applications (apps).
- Services, such as remote databases or cloud-based tools like Slack.

This password guidance is for all users.

## Best practices for everyone

The MoJ password guidance follows NCSC guidance. The NCSC recommends a simpler approach to passwords. Some agencies or bodies might have specific requirements or variations. Check your team Intranet or ask your Line Manager for more information.

Follow the CyberAware advice to generate your passwords. Always use a separate and unique password for each account or service.

The most important points to remember are that passwords should be:

- At least 8 characters long.
- No more than 128 characters long.
- Not obvious.
- Not a dictionary word. A combination of dictionary words might be suitable, such as '`CorrectHorseBatteryStaple`'.
- Unique for each account or service.

If a system or another person provides you with a password, change it before doing any MoJ work on that system. Examples of 'single-use' passwords include:

- Your own account on a work-provided laptop.
- A shared account for accessing a data analytics service.
- All supplier or vendor supplied accounts.

You must change a password whenever:

- There has been a security incident involving your account or password. For example, someone guessed your password, or you used it on another account.
- There was a security incident with the service that you access using the password. For example, if someone broke into the system that provides the service you use.
- Your line manager or other authorised person tells you to do so.

When required to change a password, you must do so as soon as possible. If you don't change the password soon enough, you might be locked out of your account automatically. The following table shows the maximum time allowed:

| Type of system | Maximum time to change a password |
|---|---|
| Single-user systems, such as laptops | 1 week |
| All other systems | 1 day |

## Password expiry

You don't have to change a password because it is old. The reason is that time-expiry of passwords is an ...outdated and ineffective practice.

Some current or legacy systems don't allow passwords that follow MoJ guidance. For example, some mobile devices, laptop hard drive encryption tools, or older computers might not be able to support a mix of character types. For such systems, choose passwords that are as close as possible to MoJ guidance.

### Password managers

Use a password manager to help you keep track of your passwords.

These are tools that help you create, use, and manage your passwords. A useful overview is available here.

As passwords become more complex, and you need to look after more of them, it becomes increasingly necessary to use a password manager. For example, development teams in MoJ Digital & Technology use LastPass.

You still need to remember one password. This is the password that gets you into the manager application. Once you have access, the application works like a simple database, storing all the passwords associated with your various accounts and services. Some managers have extra features, such as password generators. Some managers can even automatically fill-in username and password fields for you when during log in.

The password manager database is often stored in the cloud so that you can use it anywhere. The database is encrypted, so only you can open it. That's why your single password key is so important. Without it, you can never get access to the password database again.

Using a password manager for your MoJ account and service details is recommended.

You can find additional useful information about password manager tools here.

### Default passwords

Change all default passwords when a new, modified, or replacement system arrives. Complete the changes before making the system available for any MoJ work.

### Password access attempts

If a password is ever entered incorrectly, a count starts. After at most 10 (ten) consecutive failed attempts at using the correct password, access to the account or system is locked. A successful use of the password resets the count to zero again.

### Password reset

If a password lock occurs, a reset is necessary. This requires action by the system administrator or the MoJ Service Desk. The process should be like issuing the password for the first time. Other account details are not changed during the reset. This helps avoid losing any work. Checks ensure that an attacker cannot use the password reset process.

### Blocking bad passwords

You should not try and use obvious passwords. Attempts to do so will be blocked.

### Single-use passwords

Some passwords are 'one time' or single-use. Administrators and developers use these to grant access to a service for the first time. After using the password once, the user must immediately change the password.

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

The following table shows the valid lifetime of a single-use password:

| Type of system | Lifetime of a single-use password |
|---|---|
| Single-user systems, such as laptops | 1 week |
| All other systems | 1 day |

### Contact details

- Contact the Cyber Assistance Team for specific advice on IT security: CyberConsultancy@digital.justice.gov.uk.

- For any further questions relating to security, contact: security@digital.justice.gov.uk.
- To report an incident.

## Using LastPass Enterprise

### What is LastPass?

LastPass is an online password management tool that we make available to you to help you create, store and share passwords. Using it means you no longer need to remember dozens of passwords, just a single primary password. It keeps all your website logins protected, helps with creating new 'strong' passwords and password sharing when required.

LastPass is available as a browser extension for popular browsers and as well as a full software suite (for use outside of browsers) for Microsoft Windows and Apple macOS.

LastPass will securely save your credentials in your own LastPass 'Vault' and then offer to autofill those credentials the next time you need them.

The Ministry of Justice (MoJ) has the Enterprise tier of LastPass.

### Who should use it?

MoJ LastPass accounts can be requested by anyone in MoJ Digital & Technology.

At the moment, rollout is limited to technical service/operation teams but we're working on license funding to make it available to everyone in D&T.

### How to get it

Email lastpass-admins@digital.justice.gov.uk to request access.

Make sure you include in the email:

- which team you're in
- your role in your team / why you need access
- if there were any credentials within Rattic that you need access to based on this shared spreadsheet of old Rattic credentials

### What it can be used for

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

LastPass can also be used for sharing passwords within a team when individual named accounts cannot be created in the service. A good example is running a shared Twitter account.

#### *Personal use*

You could use your MoJ LastPass account to store personal non-work information but as it is a work account belonging to the MoJ you may lose access if you change role and will lose access entirely if you leave the MoJ.

MoJ LastPass administrators cannot routinely access the contents of LastPass Vaults but can reset accounts to gain access if there is a good reason to do so.

### What it shouldn't be used for

LastPass should not be used for storing MoJ documents - you must use existing MoJ services such as Office 365 or Google Workspace for that.

You shouldn't use LastPass for 'secrets' that belong to systems, only credentials to be used by humans.

### How to use it
### Getting started

You will be sent an email to your MoJ work email account inviting you to create your LastPass account. LastPass have 'getting started' guides on their website.

*Creating your primary password*

You need to create a primary password - this is the only password you'll need to remember.

It must be at least 12 characters long (the longer the better).

You can choose to make it pronounceable and memorable (passphrase) such as `CyberSecurityRules!` or `Sup3rD00p3rc0Mp3X!`, as long as you're comfortable remembering it and won't need to write it down.

There are password guidance standards on the MoJ intranet.

Your primary password **must** be unique and you should **never** use it anywhere else (including a similar version, for example, by simply adding numbers to the end)

*Multi-Factor Authentication*

You **must** setup multi-factor authentication (MFA, sometimes known as 2FA) for your MoJ LastPass account.

LastPass has a guide on setting up MFA.

If you don't have an MoJ-issued work smartphone you may use a personal device for MFA.

### Sharing passwords

To share a password create a 'shared folder' in the LastPass Vault.

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

(You must not share your LastPass main password with anyone, even your line manager or MoJ security.)

### Using it abroad

Taking a device (such as personal smartphone) that has MoJ LastPass installed counts as travelling abroad with MoJ information.

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

It may be simpler to 'log out' of the LastPass applications or uninstall/delete them before travelling outside of the UK and reinstalling when you get back.

### Keeping LastPass update to date

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

### Need help?

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

If you need help using LastPass such as getting access to shared folders or resetting your primary password as you have forgotten it, contact lastpass-admins@digital.justice.gov.uk

# Operations security

## Control of operational software

### Guidance for using Open Internet Tools

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

This guidance gives you:

- an overview of Open Internet Tools (OIT)
- a quick checklist to help you decide if you can use an OIT
- reasons why you might, or might not, want to use an OIT
- things you must think about when using an OIT, such as data protection
- information on who to contact if you would like help or advice

**Note:** To access some of the links in this guide you'll need to be connected to the MoJ Intranet

### Overview

Open Internet Tools (OITs) are applications or services from suppliers outside the MoJ. They often have the following characteristics:

- they are general purpose. This means they are not specific to the MoJ. Other organisations can use them
- they are accessed using the Internet, usually through a web browser. This means that if you have Internet access, you are able to connect to the tools
- they have a basic 'free-to-use' version. This means that you are able to use some or all the capabilities, but with some constraints. For example, an online word-processor might limit you to 5 documents in your account
- they have one or more 'paid for' versions. By paying for the tool, you unlock some or all the constraints

### Quick checklist

To help you decide if you can use an OIT to work on an MoJ task, consider the following questions:

- is the task information subject to specific rules or requirements in your part of the MoJ?
- is the task information classified as anything other than `OFFICIAL` or `OFFICIAL-SENSITIVE`?
- does the task information include any data identifiable as being about someone?
- is this the first time anyone has used the tool for MoJ business?
- does the tool need access to your account or other data you can access? For example, does it ask to use your MoJ Google or Microsoft Office account?
- does the tool install a web-browser extension?
- is the tool a plug-in for existing OITs we use, such as Slack, Confluence, or Jira?
- could there be damaging consequences if the task information you work with using the tool is:
  - lost
  - stolen
  - published in the media
- are you prevented from exporting all the data from the tool?
- are you prevented from deleting all the data from the tool when you finish working on the task?

If the answer to *any* of these questions is 'Yes', you might not be able to use the OIT.

When you have all the answers, request formal approval to use the OIT from your Line Manager. Do this *before* using the OIT.

### Why OITs are an opportunity

OITs offer some significant advantages for you and the MoJ, including:

- enabling you to work the way you want to, more effectively
- usually cheaper than buying or building and supporting a dedicated tool
- no need to build or support the tool
- good use of open standards, such as file formats
- reduced need to have specific hardware or software on computers
- rapid patching to address security issues
- easy updates and deployment of new features
- a large pool of help and support
- easy access, whenever you have a network connection
- increasing availability of some or all capabilities when disconnected from the network

### Why OITs are a risk

OITs also pose some threats or risks, including:

- dependency on the tool and supplier
- security of access to the tool
- security of information stored within or processed by the tool
- potential difficulty of enhancing or customising the tool for MoJ-specific requirements

But as long you consider the threats or risks, and address them, OITs provide many benefits for you and the MoJ.

### Summary

With careful use, OITs help you to work more effectively and efficiently. Think about them as serious and preferable options for performing tasks.

### Using OITs

This guidance helps you:

- understand the conditions or constraints that apply to a tool, or a task performed using a tool
- identify and address threats or risks posed by a new tool

### Privacy and personal information

Data protection legislation makes you responsible for personal information you work with. You must keep it safe and secure. In particular, you must follow data protection obligations. These include the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Don't use OITs for storing personal data until you have addressed the need to get consent first. Check if using the OIT might need an update to existing privacy policies or notices. Don't use OITs if unlawful disclosure of the information they process might cause damage or distress.

Data protection legislation might also limit *where* you can process personal data. An OIT should have a privacy statement that describes where it stores or processes data. Be ready to contact the OIT provider for more information about this aspect of their service.

Be sure you can fulfil your data protection responsibilities when using an OIT. It might be helpful to complete a Privacy Impact Assessment (PIA).

Complying with personal information requirements can be complex. Don't hesitate to ask for advice: privacy@justice.gov.uk

### Classification and security

An OIT can only store or process information classified at `OFFICIAL` level.

Think about the MoJ information you work with. What would happen if you lost it, or it's stolen, or published in the media? Suppose the information was overheard in a cafe, or read from your screen on a crowded train. Could there be damaging consequences? If the answer is 'No', then it's probably OK to use OITs to store or send that information.

Think also about information moving across the Internet. The data might be safe within the MoJ and in an approved OIT. But what about the connection between the two? Sending information might involve insecure networks.
Be aware of the security implications. Check that enough suitable security measures are in place to protect the information. For example, check for encryption of network connections using SSL/TLS. A simple way to do this is to look for the secure connection indicator in your web browser:


You have a duty of confidentiality and a responsibility to safeguard any HMG information or data that you access. This is Principle 2 of the Government Security Classifications. The MoJ trusts you to work with `OFFICIAL` information. In the same way, you're trusted to make a reasoned judgement about whether it's safe to use an OIT.

Useful help for deciding what is OK is in existing social media guidance. While it's more about how to act online, the principles are helpful for OITs.

Remember that it is impossible to delete information after it's released in public.

For more information about MoJ IT Security, look on the MoJ Intranet here.

### Storage and data retention

Laws and regulations make the MoJ and its employees responsible for managing information. Some examples include:

- the Freedom of Information Act
- the Data Protection Act and General Data Protection Regulation
- the Public Records Acts

When we receive a request for information, we need to know where we hold all the relevant information. Storing business information on appropriate MoJ systems helps us, because:

- we can provide evidence about decisions
- we understand the information held, and where to find it
- we can transfer records to The National Archives

Always store MoJ information in MoJ systems. If you use an OIT, make sure the key information is also stored in an appropriate MoJ system. Guidance on what you must keep is available here. At regular and convenient intervals, transfer the information to an appropriate MoJ system. Do the same when you finish the work. Don't forget to remove any redundant information from the OIT.

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

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

### Service and support

OITs are often intuitive and reliable. But that doesn't mean they are always available and always work as you expect. The MoJ can't provide technical support or ensure service availability for them. Always have another way of working if the OIT is not available for some reason or for any length of time. In other words, don't let an OIT become business critical.

Check the OIT usage agreement to find out more about the service and support available.

**Note:** The MoJ cannot provide technical support for OITs.

### Common OITs

There are already many OITs used across the MoJ. Permission to use an OIT might vary, depending on where you work in the MoJ. For example, some teams must not access or use some OITs, for security or operational reasons.

**Note:** Check with your Line Manager if you want to use an OIT for your work, *before* you use it.

### Getting help

For further help about aspects of using OITs within the MoJ, contact:

| Subject | Contact |
|---|---|
| Classification and Security | MoJ Cyber Security team |
| Storage and Data Retention | Departmental Library & Records Management Services (DLRMS) |
| Information Assurance | Compliance and Information Assurance Branch |

| Subject | Contact |
|---|---|
| Personal Data | Disclosure Team |

Last updated: April 16th, 2020.

# Communications security

## Information transfer

### Bluetooth

#### Introduction

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

Bluetooth is a very short range WiFi technology. In everyday terms, Bluetooth devices can 'talk to each other' if they are very close, for example in the same room. This makes Bluetooth really good for wireless devices, for example a telephone headset, or a mouse or keyboard.

Bluetooth works by 'pairing' devices. This makes it quick and simple to use. The problem is that Bluetooth, and the pairing process, is not very secure. This means that attackers might get unauthenticated access to devices. As an example, an attacker 'listening' to the Bluetooth connection between a computer and a keyboard could possibly intercept passwords or other sensitive information as the details are typed on the keyboard.

This guidance tells you more about the Ministry of Justice (MoJ) view of Bluetooth, from a security perspective. It also gives you hints and tips on how to use Bluetooth more safely.

The aim is to help you maintain the Confidentiality, Integrity and Availability of MoJ data, applications and services. The results should be that:

- the information you access is not compromised
- you can connect devices using Bluetooth, safely
- you are aware of the problems around Bluetooth, and can take the necessary safety precautions

**Note:** Remember that there might be local rules that apply regarding the use of Bluetooth devices. A good example is in Prisons, where use of Bluetooth would not be available by default. Ensure that you check with local requirements.

#### Accessibility

Some types of Bluetooth devices are not allowed, by default. However, where there is a good reason for requiring a Bluetooth device, such as for Accessibility reasons, then a request for an exception to use the device will be treated sympathetically and permitted wherever possible.

Contact the Cyber Assistance Team by email: CyberConsultancy@digital.justice.gov.uk

#### Bluetooth devices and risks

Examples of Bluetooth devices, and whether they might be used for business purposes, are as follows:

| Bluetooth device | Suitable for MoJ work purposes (Y/N) |
|---|---|
| Keyboards | Y |
| Mouse | Y |
| Telephone headsets | Y |
| Headphones | Y |

| Bluetooth device | Suitable for MoJ work purposes (Y/N) |
|---|---|
| Earbuds | Y |
| Trackpads | N - but exception possible for Accessibility reasons |
| External speakers | Y - but be aware of other people or devices nearby that might be listening |
| Gaming joysticks and controllers | N - but exception possible for Accessibility reasons |
| Laptops | Y - for MoJ-issued devices |
| Hearing aids | Y |
| Watches and Fitness bands | N |
| Smart TVs | N - requires authorisation |
| Storage devices (similar to USB 'thumb' drives) | N |
| Internet-of-things 'Smart speakers' | N |

A Bluetooth device might be at risk from any of the following:

- Eavesdropping
- Unauthorised access
- Message modification
- Denial of service
- Data exfiltration
- Insecure data transmission
- Phishing

An example of a Bluetooth problem is 'bluetooth marketing'. As your walk around with your mobile phone, it is continuously looking for Bluetooth devices and WiFi access points. It does this to help with acurate location tracking. But other devices can also see your mobile phone. These devices might report tracking information about where you were at any time. This guidance will help you understand more about the problem, and suggest things you can do to reduce the risks.

### Best practices for using Bluetooth

Before using a Bluetooth device in a work context, consider the following:

- What is the business case for using the Bluetooth device?
- What data might be or will be access through, or using, the Bluetooth device?
- Does the Bluetooth device have the latest patches and fixes applied - where possible?
- Was the Bluetooth device purchased from a reputable vendor?
- Does the Bluetooth device require a PIN code or similar before connecting?
- Are the Bluetooth devices 'discoverable'?
- Have you connected to any other 'public' Bluetooth devices?
- Are all the devices password protected?
- Might someone be able to see what Bluetooth devices you are using?
- Is the material you are working with `OFFICIAL-SENSITIVE` or higher?

The best way to ensure your Bluetooth device is as up-to-date as possible is to apply all patches and fixes for all hardware devices as soon as you can.

Bluetooth is a very cheap and simple technology. This means that it is often included in extremely cheap devices; often these use old versions of technology or are not provided with patches and fixes. The best thing is to obtain any Bluetooth devices from reputable vendors, so that it is more likely the device will be supported and maintained correctly.

Many Bluetooth devices try and make connection as easy as possible by enabling 'Direct Connection'. This often means that you only need to 'find' a Bluetooth device on your 'phone or laptop, then click once for a connection to be established. While very easy, this is not safe, because those same direct connections can also happen automatically, 'behind the scenes', without you being aware. If possible, ensure that a Bluetooth connection is allowed only when a PIN or password is supplied. This reduces the risk of 'hidden' Bluetooth connections.

Some Bluetooth devices allow you to choose whether they are 'discoverable'. For example, on Android 'phones, you can go to the `Settings -> Connected devices -> Connection preferences -> Bluetooth visibility` or similar. The best advice is to change the Bluetooth settings to undiscoverable if you can. Only make the device discoverable when you need to connect to a trusted device.

At regular intervals, check to see what Bluetooth devices are 'known' to your devices. Remove any you don't recognise.

When in public places, make sure you only connect to known devices. Always ensure you are in a secure and safe location such as home, office, or a known isolated place before switching on your Bluetooth.

If someone can see what Bluetooth devices you have, or are using, they might try and use one of their device to intercept or monitor the connection. Try to keep Bluetooth devices out of sight so that no-one knows which ones you might actually be using. Even the bright blue light Bluetooth devices illuminate when they are connected might draw unwanted attention.

Generally speaking, Bluetooth devices do not present extra problems when working with `OFFICIAL` material. However, the whole point of Bluetooth is to enable and simplify communications, so you need to be extra careful when using Bluetooth devices while working on `OFFICIAL-SENSITIVE` or higher material.

### Getting more help

Contact the Cyber Assistance Team by email: CyberConsultancy@digital.justice.gov.uk

## Email security

### Overview

This document provides you with guidance for safe and secure use of email within the Ministry of Justice (MoJ).

In general, always use email in an acceptable way.

In particular:

- Never circulate messages or material that contains obscene, profane, inflammatory, threatening, harassing (racially, sexually or otherwise), and disruptive, or otherwise offensive language.
- Don't use email or other messaging systems for trivial debates or exchanges with an individual or group of people.
- Don't use MoJ email or other messaging systems for anything other than appropriate business purposes.
- Don't make statements that defame, slander or lower the reputation of the MoJ, any person or organisation.
- Don't forward email chain letters to your contacts. Instead, report them to security@digital.justice.gov.uk.
- Avoid excessive use of email. Be aware of unsuitable attachments, for example video clips, images, or executable files.
- Avoid sending email to large numbers of recipients. Ask yourself if it really makes sense to "Reply All"?.

Be aware that the MoJ monitors the use of electronic communications and web-browsing. Your manager can request reports detailing your activity if they suspect inappropriate use of email or web-browsing facilities.

For further information, ask your manager or contact your local IT help desk.

Suppliers to the MoJ should first ask their usual MoJ points of contact.

### Email threats

Although email is a powerful business tool, it has problems. In this guidance, we describe some of the problems, and how you can avoid them.

Email threats often use familiar email addresses to disguise attacks, or to pose as valid emails. Email threats are becoming more frequent and pose one of the biggest problems for MoJ systems and services.

There are many possible threats, including:

- Viruses: These can be spread between computers in emails or their attachments. They can make PCs, software or documents unusable.
- Spam: This is unsolicited mail sent in bulk. Clicking on links in spam email may send users to phishing websites or sites hosting malware. Often email spam mimics the addresses of people you know.
- Phishing: These are emails disguised to look like a legitimate company or bank to illegitimately obtain personal information. They usually ask you to verify your personal information or account details. Often links will direct you to a fake website, made to look like the real thing.
- Social engineering: In the context of security, social engineering refers to manipulating people to do something or divulge confidential information. For example, you might get a call from someone pretending to be from a software supplier, claiming that a virus has been found on your PC; they demand personal details before they can remove the virus.
- Spoofing: A spoofed email is where the sender (in this case, a criminal) purposely alters part of the email to make it look as though it was from someone else. Commonly, the sender's name/address and the body of the message are made to look as though it was from a legitimate source. It is commonly used to trick the recipient into providing confidential information such as passwords, or to market an online service dishonestly, or to sell a bogus product. Check the real sender of any email you receive if you ever have any doubt or uncertainty. If the sending address is one you don't recognise, do not click on any link contained within the email.

The MoJ scans approximately 10 million messages a month for threats. Of these, we might expect to find 600,000 spam messages and 23,000 virus messages. Unfortunately, not every virus or spam email will be identified and blocked. The good news is that there are some simple steps you can take to reduce the threat:

- If you are not expecting the email, do not reply to it.
- If you are at all suspicious, do not divulge your details or any sensitive information.
- Avoid opening potential scam emails. This may alert the 'scammer' you have viewed their message.
- Don't open unexpected attachments or click on strange links in emails, even if the email appears to be from someone you know. Check the style and content; if it isn't consistent with previous emails, it could be a scam.
- Do not reveal personal or other sensitive information in response to automatic email requests.
- Avoid sharing your business email address on the internet. These might be collected and used by automatic 'harvesting' software programs.
- Never use your MoJ email address to register for non-work related sites.

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

### Further reading from the NCSC

Email security and anti-spoofing

### Other email problems

### Auto-forward

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

But auto-forwarding is very risky.

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

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

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

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

There might be occasions when you have a genuine business need to auto-forward email to another email account, where the new address has the same or higher security standards. An example is forwarding from an MoJ business email address to another MoJ business email address. If you have business need for this, contact the Operational Security Team to discuss your requirements: OperationalSecurityTeam@justice.gov.uk.

### Chain letters

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

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

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

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

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

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

*When in doubt, don't send it out.*

### Scams

Scams are "get rich quick" schemes. They make claims such as promising your bank account will soon be stuffed full of cash if follow the detailed instructions in the letter or email. In reality, it is an illegal plan for making money.

A typical scam includes the names and addresses of several individuals whom you may or may not know. You are instructed to send a certain amount of money to the person at the top of the list, and then remove that name and add yours to the bottom.

You are then supposed to mail copies of the letter or email to a few more individuals who will hopefully repeat the entire process. The letter promises that if they follow the same procedure, your name will gradually move to the top of the list and you'll receive money.

Other high-tech scams using IT also exist. They might be sent over the internet, or may require the copying and mailing of computer disks rather than paper. Regardless of the technology used to advance the scheme, the end result is still the same.

Scams are a bad investment. You certainly won't get rich. You will receive little or no money. The few pounds you may get will probably not be as much as you spend making and mailing copies of the letter if hard copy.

By their very nature, scams are harassing. Sending such mails using MoJ facilities is prohibited. The misuse of computer resources to harass other individuals or groups is unacceptable. Any person tempted to forward an email scam should familiarise themselves with the HR intranet pages, particularly the section regarding disciplinary action and electronic communications.

*Scams also clog up the system and reduce the efficiency of our servers.*

#### *How to recognise a scam*

From the older printed letters, to the newer electronic kind, scams follow a similar pattern, with three recognisable parts:

- A hook: this to catch your interest and get you to read the rest of the letter. Hooks used to be "Make Money Fast" or "Get Rich" or similar statements related to making money for little or no work. Electronic chain letters also use the "free money" type of hooks, but have added hooks like "Danger!" and "Virus Alert" or "A Little Girl is dying". These tie into our fear for the survival of our computers or into our sympathy for some poor unfortunate person.
- A threat: when you are hooked, you read on to the threat. Most threats used to warn you about the terrible things that will happen if you do not maintain the chain. Others play on greed or sympathy to get you to pass the letter on. The threat often contains official or technical sounding language to get you to believe it is real.
- A request: some older chain letters ask you to send money to the top ten names on the letter and then pass it on. The electronic ones simply admonish you to "Distribute this letter to as many people as possible." They never mention clogging the internet or the fact that the message is a fake; they only want you to pass it on to others.

If it sounds too good to be true, then it is!

### Bogus calls

There are a range of scams that can target you at home or at work. Callers usually say they are from IT Support, and tell you that they have detected a virus on your machine that needs to be removed. The bogus caller will then either:

- Direct you to a website, in the hope you will download malicious software.
- Try and obtain details from you about your computer, or the MoJ network.

In all genuine situations, the MoJ service desk will provide you with an incident reference number if there is a real problem with your machine.

If you receive a call from someone claiming to be from the service desk, *always* ensure you ask them for the incident reference number. Then disconnect the call, and call service desk yourself, directly. If the original call was genuine, when you provide the incident reference number, they will be able to help you.

In general:

- Treat all unsolicited calls as suspicious.
- If possible, note the details and incoming telephone number of the caller.
- Do not go to any external site if directed from an unsolicited call.
- Never give any information about your computer to the caller.
- Check if the call is genuine with your IT Service desk. Report the call as a security incident if it is not. Use a different phone from that used to take the original call.

### Hoaxes

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

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

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

#### *The risk and cost of hoaxes*

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

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

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

### *How to recognise a hoax*

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

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

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

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

### *Type of hoaxes*

Scam chains

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

Giveaways

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

Malicious warnings (virus hoaxes)

Warnings about Trojans, viruses, and other malicious code that have no basis in fact, for example `Jdbgmgr.exe`.

Virus hoaxes have flooded the internet with thousands of viruses worldwide. Paranoia in the internet community fuels such hoaxes. An example of this is the "Good Times" virus hoax, which started in 1994 and is still circulating the internet today. Instead of spreading from one computer to another by itself, Good Times relies on people to pass it along.

Sympathy letters and requests to help someone

Requests for help or sympathy for someone who has had a problem or accident.

Urban myths

Warnings and stories about bad things happening to people and animals that never really happened.

Inconsequential warnings

Out of date warnings and warnings about real things that are not really much of a problem.

True legends

Real stories and messages that are not hoaxes but are still making the rounds of the internet.

Traditional chain letters

Traditional chain letters that threaten bad luck if you do not send them on or request that you send money to the top *x* people on the list before sending it on.

Threat chains

Mail that threatens to hurt you, your computer, or someone else if you do not pass on the message.

Scare chains

Mail messages that warn you about terrible things that happen to people (especially women).

Jokes

Warning messages that it's hard to imagine anyone would believe.

### Email and storing MoJ information

Data held by the MoJ should be managed in such a way that employees who require the data, for business reasons, can gain access to it. Managers should ensure that data is stored in an area that is easily accessible to those who require access. This includes MoJ information exchanged using email.

If you need further assistance or information about this process, email Operational Security: OperationalSecurityTeam@justice.gov.uk.

### Accessing emails or information in an absent employee's email account

Staff absences do occur and these can cause disruption to MoJ business where colleagues have no access to relevant departmental information. Unfortunately, some staff go on annual leave, secondment or maternity leave, but don't make provision for colleagues to access departmental information.

When an absence occurs, there is *no* right to be able to access another employee's account to obtain information. This is true, regardless of whether the absence is expected or unexpected, for example annual leave or illness.

Accessing another employee's account, without their permission, might contravene data protection legislation.

Data protection legislation protects personal information which relates to identifiable, living individuals held on computers. It specifies that appropriate security measures must be in place to protect against unauthorised access to, loss or destruction of personal data. If you breach this principle you could render the MoJ liable to enforcement action by the Information Commissioner.

There are limited circumstances in which it is possible to gain lawful access to another employee's email account. These include:

- A criminal investigation by a law enforcement agency.
- To enable an IT Misuse investigation to be carried out providing it is conducted using appropriate policies.
- On the death of an employee, as data protection legislation no longer applies.

### Contact details

- Contact the Cyber Assistance Team for specific advice on IT security: CyberConsultancy@digital.justice.gov.uk.
- For any further questions relating to security, contact: security@digital.justice.gov.uk.
- To report an incident.

## General Apps Guidance

### Overview

When working from home, you still need to communicate with Ministry of Justice (MoJ) colleagues. You'll also need to work with people outside the MoJ. There are various tools you might use, besides the standard email and telephone tools. This document tells you about the tools you can, and cannot, use for business purposes. This guidance applies to all staff and contractors who work for the MoJ.

Some ALBs, Agencies, or other large groups within the MoJ might have their own, specific guidance regarding how to use certain Video and Messaging apps for different purposes.

### Access to tools

You can access tools that are provided through your MoJ provided devices by downloading from:

- The Software Centre application on your device (for Dom1 equipment).
- The Self Service application on your Mac (for Digital Service Desk (DSD) managed MacBook laptops).

Currently, access to the tools mentioned in this document is not available from Quantum devices.

For other MoJ provided devices, seek help from your Line Manager in the first instance.

### Corporate, work and personal accounts

- A corporate account is for making official MoJ statements and providing official views. Only a small number of authorised people can use it.
- A work account is your normal MoJ account, that you use every day for business as usual. Only you have access to your work account.
- A personal account is your own personal account on gmail, hotmail, yahoo, and so on. You should never use a personal account for business purposes.

Some of the applications listed make a distinction between general use with a work account, and use with a corporate account. Using a tool with a corporate account means you are providing views or statements on behalf of the MoJ. Never use a personal account for business purposes with any tool.

Remember that if you are authorised to use a corporate account, you are speaking and acting for the whole of the MoJ. When working with a personal account, you are speaking and acting as an MoJ employee and a civil servant.

Always follow all MoJ policies and guidelines regarding public information, including social media (to access this information you'll need to be connected to the MoJ Intranet). In particular, follow the Civil Service Code of Conduct.

### Using video conference tools safely

The NCSC has excellent guidance on using video conferencing services safely.

Key things to remember *before* a call include:

- Make sure your video conferencing account (or the device or app you are using for video conferencing) is protected with a strong password.
- Test the service before making (or joining) your first call.
- Understand what features are available, for example recording the call or sharing files or screen information.

Key things to remember for *every* call include:

- Do not make the calls public, for example always require a password to join the call.
- Know who is joining the call, in particular check that everyone is known and expected to be present, and that people who have dialled in have identified themselves clearly and sufficiently.
- Consider your surroundings, for example checking what can be seen behind you (forgetting to check information on a whiteboard or noticeboard is an easy mistake).

## MoJ Policy and guidance

### `OFFICIAL` and `OFFICIAL-SENSITIVE` Information

`OFFICIAL` information is the majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

`OFFICIAL-SENSITIVE` is not a classification. `SENSITIVE` is a handling caveat for a small subset of information marked `OFFICIAL` that requires special handling by staff. You should apply the handling caveat where you wish to control access to that information, whether in a document, email, or other form.

### Privacy and personal information (Data Protection)

Some communications tools expect to have a copy of your contacts list. The list is uploaded to the tool server in order to let the tool to function correctly. Think carefully about whether this is reasonable to do. Make sure that sharing your contacts list does not impact any one else's privacy in a negative way.

Data protection legislation makes you responsible for personal information you work with. You must keep it safe and secure. In particular, you must follow data protection obligations. These include the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Complying with personal information requirements can be complex. Don't hesitate to ask for advice:

- Email: privacy@justice.gov.uk
- Slack: `#securityprivacyteam`

- Intranet: https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/

### Information Management

Many of the tools are only used for your day-to-day communication with colleagues. The information you work with is typically classified at OFFICIAL.

Think about the MoJ information you work with when using these tools. What would happen if you lost your mobile device, or it's stolen? Suppose the voice or video call was overheard in a cafe, or read from your screen on a crowded train. Could there be damaging consequences? If the answer is 'No', then it's probably OK to use the tool to communicate that information with colleagues.

You have a duty of confidentiality and a responsibility to safeguard any HMG information or data that you access. This is Principle 2 of the Government Security Classifications. The MoJ trusts you to work with OFFICIAL information. You're trusted to make a reasoned judgement about whether it's safe to use an approved tool, or whether you should use a different MoJ-provided work tool.

Remember that it is impossible to delete information after it's released in public.

For more information about MoJ IT Security, look on the MoJ Intranet here.

### Storage and data retention

Laws and regulations make the MoJ and its employees responsible for managing information. Some examples include:

- Freedom of Information Act.
- Data Protection Act and General Data Protection Regulation.
- Public Records Acts.

When we receive a request for information, we need to know where we hold all the relevant information. Storing business information on appropriate MoJ systems helps us, because:

- We can provide evidence about decisions.
- We understand the information held, and where to find it.
- We can transfer records to The National Archives.

Always store MoJ information in MoJ systems. If you use a tool for work tasks, make sure the key information is stored in an appropriate MoJ system. Guidance on what you must keep is available on the Intranet here. At regular and convenient intervals, transfer the information to an appropriate MoJ system. Do the same when you finish the work. Don't forget to remove any redundant information from a tool by clearing or deleting data if it has been preserved in an MoJ system.

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

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

### Acceptable Use

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

Be sensible when using communications tools for MoJ business purposes:

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

The bottom line is: *"if there is doubt, there is no doubt - ask for help"!.*

### Approved tools

| Tool name | Tool type | Conditions/ constraints on use | Accessing /installing tool | Audience |
|---|---|---|---|---|
| Apple Facetime | Communication tool: Video | Avoid personal or sensitive data | Smartphone App | Internal/ External |
| Apple iMessage | Text messaging | Avoid personal or sensitive data | Smartphone App | Internal/ External |
| Google Hangouts | Communication tool: Video and/or voice | MoJ use approved | Digital Service Desk controlled Mac - Self | Internal/ External |
| Microsoft Teams | Communication and collaboration tool: Video and/or voice | MoJ use approved | Dom1 Software centre, Digital Service Desk controlled Mac - Self service, Web browser. | Internal/ External |
| Miro | Collaboration tool: Whiteboarding | Avoid personal or sensitive data | Web browser. | Internal/ External |
| Skype for Business | Communication tool: Video and/or voice | MoJ use approved | Dom1 Software centre, Digital Service Desk controlled Mac - Self service, Web browser. | Internal/ External |
| Slack | Text messaging, Voice/ Video calls, etc. | Avoid personal or sensitive data | Digital Service Desk controlled Mac - Self service, Web browser. | Internal/ External |
| Slido | Q&A tool during presentations | Avoid personal or sensitive data | Web browser | Internal |
| Twitter | Text Messaging, Video transmission | Approved for MoJ Corporate account. Using a personal account to comment on work related issues is encouraged, as long as you follow the Civil Service Code of Conduct. | Web browser, Windows 10 App, Smartphone App | Internal/ External |
| WhatsApp | Text messaging, Voice/ Video calls | Avoid personal or sensitive data | Dedicated app on device, also web browser. | Internal/ External |
| Yammer | Text messaging | Avoid personal or sensitive data | Dedicated app on device | Internal |
| YouTube | Video sharing tool: Video, streaming and chat | Avoid personal or sensitive data | Web/browser based use | Internal/ External |
| Zoom | Communication tool: Video, voice and chat | Avoid personal or sensitive data | Web/browser based use | External meetings |

### NHS Track and Trace

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

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

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

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

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

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

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

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

#### Other tools

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

If you wish to use a tool that is not listed above, please consult our Guidance for using Open Internet Tools and speak to us for help.

#### Requesting that a tool be approved for use

Refer to the Guidance for using Open Internet Tools for the process to follow when wanting to add a new tool to the list.

#### Other information
#### Government policy and guidance

GDS Social Media Playbook

#### NCSC

Video conferencing services: using them securely

Secure communications principles

Using third-party applications

# Information security incident management

## Management of information security incidents and improvements

### Lost Laptop or other IT security incident

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

#### What to do if your device is lost, stolen, or compromised

If MoJ data or information is lost or compromised, you should always report it as a data incident.

**Note:** You can help reduce problems by making sure that devices used for MoJ tasks are always shut down before leaving Government premises. Locking a laptop, or 'putting it to sleep' is not completely secure. A lost or stolen laptop can be accessed more easily if it is only locked or sleeping. A shut down makes sure that all security measures are in place, such as full disk encryption.

If you think your device is lost, stolen, 'hacked', or in some way compromised, you must:

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

   **Dom1/Quantum - Technology Service Desk**

   - Tel: 0800 917 5148

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

   **Digital & Technology - Digital Service Desk**

   - Email: servicedesk@digital.justice.gov.uk
   - Slack: `#digitalservicedesk`
2. Tell your line manager as soon as possible.
3. For a lost or stolen device, contact the Police and make sure you get the incident reference number.

### Summary

Find out more about how to report a security incident here.

# Compliance

## Compliance with legal and contractual requirements

### Data security and privacy

#### Data Security and Privacy

We believe that our technology must keep data safe and protect user privacy.

Our digital projects contain important information. Serious data breaches might result if we fail to:

- protect information
- handle it correctly at all times
- dispose of it safely when it is no longer required

Breaches might cause:

- harm to individuals
- financial loss to the Ministry of Justice (MoJ)
- a loss of confidence in us as an organisation

For personal data, the EU General Data Protection Regulation (GDPR) and UK Data Protection Act (2018) apply. These make the consequences of data breaches very clear.

To follow the data regulation/legislation, we **must** ensure that:

- we protect data to the best of our organisation's capabilities
- we collect data only for described, lawful purposes
- we use data only for the described, lawful purposes

#### Why are security and privacy important?

Breaches can have an adverse effect the relationship between citizen and government.

Not only do we have a duty to protect citizens data, but the penalties for violations are also severe. Under the GDPR, serious infringements can result in fines of up to €20M.

We must apply appropriate security and privacy protection to all the information we hold and process, at all times.

We should treat all data as sensitive unless proven otherwise.

All our work must follow this ethos.

### When this applies

This principle applies to **all** MoJ technology projects and business actitivies.

While GDPR applies only to personal information, all MoJ projects and tasks must have excellent data security and privacy characteristics. If they handle personal data, they must do so correctly. Projects must follow MoJ guidelines unless exceptional and approved circumstances apply.

The Information Commissioner's Office (ICO) - the UK's independent regulatory office for data protection - has published guidance on how to determine what is personal data.

A Data Protection Impact Assessment (DPIA, formerly commonly known as a Privacy Impact Assessment or PIA) is required for all projects. There are some exceptions described by the ICO.