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: 18 August 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 18 September 2020. For the latest, current version of the guidance, see here.

Structure

The documents are listed in the next section.

Document List

Level 1	Level 2	Documents	Target Audience
Cyber	Access Control		
		Accessing MoJ IT Systems From Abroad	All users
		Minimum User Clearance Levels Guide	All users
	Asset Management	General User Video and Messaging Apps Guidance	All users
		Guidance for using Open Internet Tools	All users
		Security Guidance for Using a Personal Device	All users
		Remote Working	All users
		General advice on taking equipment abroad	All users
Technical	Principles	Data Security and Privacy	All users
		IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER	All users

Standards

Authentication, Authorisation & Accounting

- Accounting

- Authentication
- Authorisation

Guides

General guides

- Personnel security clearances
- Cyber Security Consultancy Team: asking for help

Product specific guides

- Using LastPass Enterprise

Mythbusting

- OFFICIAL and OFFICIAL-SENSITIVE

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.

Getting in touch

Contact information

- Email
- Reporting an incident

Cyber

Access Control

Accessing 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 MOJ Security, 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 Operational Security.
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

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. This is a sub-page to the Access Control Guide.

Minimum user clearance requirements

Most of the MoJ's IT systems are able to process `OFFICIAL` information. Therefore all roles in the MoJ require staff to attain Baseline Personnel Security Standard (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.

Contact details

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

Asset Management

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 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 contact number is:

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 have some functionality (i.e. your BlackBerry will work as a mobile phone), the device 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 - 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`

General User Video and Messaging Apps Guidance

Overview

When working from home, you still need to communicate with 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 (information on a whiteboard 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:

- 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 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
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

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

Last updated: April 22nd, 2020.

Guidance for using Open Internet Tools

This information applies to all staff and contractors who work for the 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:

data.compliance@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
Personal Data	Disclosure Team

Last updated: April 16th, 2020.

Security Guidance for Using a Personal Device

Summary

Not everyone has access to an 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.

Remote Working

Key points

- Be professional, and help keep 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 Ministry of Justice (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 - 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.

Technical

Principles

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 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** technology projects.

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

You can design your product to handle personal information correctly. There are a small number of extra steps you will have to take. Remember that personal data includes anything which might identify an individual. Even online identifiers, such as cookies, are personal data.

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.

IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

The 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.

Standards

Authentication, Authorisation & Accounting

Accounting

The base principle

Any access, and subsequent activity, to any system or data **must** employ adequate accounting techniques to ensure events can be attributed to the authenticated entity.

Accounting information must be stored in a way that it cannot be readily manipulated, particularly by the authenticated entity.

Log data security & governance

Log data can include Personal Data or inadvertent sensitive data (when an application or system is unexpectedly verbose) and must be adequately protected and governed in a comparable way to the original system's data.

Security-related log data retention

Log data created and processed for information security purposes should be retained for no longer than 2 (two) years by default (this is subject to any legislative or regulative compliance requirements) but for a minimum of 6 months.

These times are generalistic as a guide, and require contextual analysis particularly where Personal Data is involved.

Authentication

The base principle

Any access to any data **must** employ adequate authentication techniques to identify the system or user to a suitable level of confidence for the system or data within.

Passwords

Where appropriate, passwords should be used as a knowledge-based factor for authentication.

MOJ has published the MOJ Password Standard.

Named individual accounts

Human user access must have unique, named and private accounts issued (with shared accounts being a rare, intentional and considered exception to this rule).

For example: Jonathan Bloggs is issued with a user account only Jonathan uses and may access.

Account sharing

Accounts must not be shared unless they are defined as shared accounts, where additional authentication and authorisation techniques may be required.

For example:

- individuals must not share a 'root' account, but be issued named accounts with appropriate privileges instead;
- Individuals must not share a single Secure Shell (SSH) private key, but generate private and individual keypairs and their public key associated to locations where authentication is required.

System-system accounts

Accounts designed for programmatic or system/service integation must be unique for each purpose, particularly in separation between different environments - such as pre-production and production.

System-system accounts must be protected against human intervention.

Token-based methods are preferred over static private key methods.

Multi-Factor Authentication

Where appropriate, multi-factor authentication (MFA) should be used as a knowledge-based factor for authentication.MFA is sometimes referred to as Two-Factor Authentication (2FA).

MoJ guidance on MFA is available here.

MFA for Administrators

Administrative accounts **must** always have MFA, unless impractical to do so. Ensure there are techniques in-place such that MFA is always enabled and active for each account.

MFA for important or privileged actions

MFA should be re-requested from the user for important or privileged actions such as changing fundemental configurations such as registered email address or adding another administrator.

MFA can also be used as a validation step, to ensure the user understands and is confirming the action they have requested, such as an MFA re-prompt when attempting to delete data.

IP addresses
Trusting IP addresses

IP addresses in and of themselves do not constitute authentication but may be considered a minor authentication *indicator* when combined with other authentication and authorisation techniques.

For example, traffic originating from a perceived known IP address/range does not automatically mean it is the perceived user(s) however it could be used as an indicator to *reduce* (not eliminate) how often MFA is requested *within* an existing session.

IP address for non-production systems

IP addresses access control lists (and/or techniques such as HTTP basic authentication) should be used to restrict access to non-production systems you do not wish general users to access.

H/T https://medium.com/@joelgsamuel/ip-address-access-control-lists-are-not-as-great-as-you-think-they-are-4176b7d68f20

Authorisation

The base principle

Any access to any data **must** employ adequate authentication techniques to identify the system or user to a suitable level of confidence for the system or data within.

Least privilege principle

The principle of least privilege (PoLP; also known as the principle of least authority) is effectively conferring only the minimum number of required privileges required in order to perform the required tasks.

This helps reduce the "attack surface" of the computer by eliminating unnecessary privileges.

Day to day examples include: not ordinarily using an 'administrator' login on an end-user device (such as a laptop), logging into a server as 'root' or a user being able to access all records within a database when they only need to access a subset for their work.

Administrator definition

An administrator is much broader than a technical system administrator to a server, network or service (such as 'domain admin' in Microsoft Active Directory) but someone has who has higher levels of access or control than a required for day to day operation.

Examples include those with high privileges on a MOJ github.com repository and credentials to the MOJ communications accounts (such as social media).

AWS assume-role

Amazon Web Services (AWS) Identity and Access Management (IAM) has a `Role` function, which effectively allows explicitly permitted and explicitly denied activity (within the AWS ecosystem) to be defined on a per role-based.

This allows IAM accounts to be grouped based on role and purpose. This avoids individual IAM accounts being given permissions individually, which can often lead to over or under priviledge configurations.

Where possible, IAM Roles should be used.

IP addresses

IP addresses in and of themselves do not constitute authentication but may be considered a minor authentication *indicator* when combined with other authentication and authorisation techniques.

For example, traffic originating from a perceived known IP address/range does not automatically mean it is the perceived user(s) however it could be used as an indicator to *reduce* (not eliminate) how often MFA is requested *within* an existing session.

H/T https://medium.com/@joelgsamuel/ip-address-access-control-lists-are-not-as-great-as-you-think-they-are-4176b7d68f20

Guides

General Guides

Personnel security clearances

Baseline Personnel Security Standard (BPSS)

Unless otherwise agreed formally by 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.

MOJ does **not** have a standing requirement for system administrators or application developers to maintain Security Check (SC).

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 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 data.compliance@justice.gov.uk.

The consultant 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.

Product specific guides

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 master 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 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 G-Suite for that.

You shouldn't use LastPass for 'secrets' that belong to systems, only credentials to be used by humans. There is separate guidance on how to handle screts.

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 master password

You need to create a master 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 master 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.

The MOJ has an 'order of preference' for which types of MFA to use:

- Hardware-based (for example, Yubikeys)
- Software-based (for example, Google Prompt on a mobile device)
- TOTP-based (the code is held by a dedicated app such as Google or LastPass Authenticator on a mobile device)
- SMS-based (a one-time code sent via SMS)

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 master 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 master password as you have forgotten it, contact lastpass-admins@digital.justice.gov.uk

Mythbusting

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.

Getting in touch

Contact information

Email

The MOJ D&T Cybersecurity team can be reached via cybersecurity@digital.justice.gov.uk.

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

Reporting an incident

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.