# Accessing MoJ IT systems overseas

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

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

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

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

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

## Steps to follow before travelling

### Part One

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

* Argentina, Armenia, Azerbaijan, Belarus, China (including Hong Kong), Egypt, Estonia, Georgia, India, Indonesia, Iran, Israel, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, the northern area of the Republic of Cyprus, North Korea, Pakistan, Russia, Saudi Arabia, South Africa, South Korea, Syria, Turkey, Turkmenistan, UAE, Ukraine, Uzbekistan.

1. Proceed directly to [Part Two](#part-two) of this process if you are national security cleared to SC or DV levels.
2. If you are subject to STRAP briefing and intend to travel to or through countries not in Western Europe, North America, Australia, or New Zealand, proceed directly to [Part Two](#part-two) of this process, and notify the STRAP team at [STRAPTeam@cluster2security.gov.uk](mailto:STRAPTeam@cluster2security.gov.uk).
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](#international-roaming).

### Part Two

1. Collect the following information:
   * Name.
   * Email address.
   * Your business area.
   * Your Security Clearance.
   * The network you use to access MoJ data, services or applications, for example DOM1 or Quantum/MoJO, or online services such as AWS or Google Workspace.
   * The make/type of equipment you want to take with you.
   * Asset Tag details.
   * Countries you’ll be visiting or passing through.
   * Dates of travel.
   * Transport details where possible, for example flights or rail journeys.
   * Proposed method of connecting, for example MoJ VPN, Global Protect VPN (for Macs), WiFi, or Mobile Data (3G/4G/5G).
   * Reason for maintaining access while overseas.
   * The MoJ data, applications, or services you expect to access during your trip.
   * Who you are travelling with.
2. The next step depends on your MoJ business area:
   * If you are part of MoJ HQ, HMPPS HQ, HMCTS, or NPS, contact your Senior Line Manager and ask for approval to take MoJ equipment overseas and access MoJ services. Ask for any special details or considerations that apply to your proposed travel arrangements. Keep a note of the answers you get.
   * If you are part of HMPPS (but *not* HQ), contact your Governor and ask for approval to take MoJ equipment overseas and access MoJ services. Ask for any special details or considerations that apply to your proposed travel arrangements. Keep a note of the answers you get.
3. Fill in the [overseas travel form](https://intranet.justice.gov.uk/documents/2020/03/overseas-travel-form.docx).
4. Send the completed form to [security@justice.gov.uk](mailto:security@justice.gov.uk), including the answers obtained from the earlier parts of this process.
5. Your request will be considered, and an answer provided, as quickly as possible.
6. When you have received all the approvals, send a copy of your request and the approvals to [OperationalSecurityTeam@justice.gov.uk](mailto: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](#international-roaming).
9. Take a copy of this guidance; it includes useful contact details that help in the event of a problem while travelling.

## International Roaming

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

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

**Note:** International Roaming can be found on [Service Now](https://mojprod.service-now.com/moj_sp/?id=home) using: **Home** > **Order IT** > **Telephony** > **Mobile Devices** > **Request for International Roaming**.

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

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

If any security-related incident occurs overseas, regardless of whether it involves MoJ equipment, you should contact the [Operational Security Team](#contacts) as soon as possible. See the guidance on [Reporting a Security Incident](https://intranet.justice.gov.uk/guidance/security/report-a-security-incident/) on the MoJ Intranet. This includes information on reporting an incident outside of UK working hours. For convenience, the out-of-hours telephone number for reporting incidents is repeated [below](#information-incident-reporting-line).

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

## Related pages

* [Taking equipment overseas](https://intranet.justice.gov.uk/guidance/security/it-computer-security/accessing-moj-it-systems-overseas/taking-equipment-overseas/)
* [Overseas travel](https://intranet.justice.gov.uk/guidance/security/travelling-abroad-business-or-personal/)
* [Staff security and responsibilities – during employment](https://intranet.justice.gov.uk/guidance/security/staff-security-and-responsibilities/during-employment)

## External websites

* [Foreign & Commonwealth Office – travel & living abroad](https://www.gov.uk/browse/abroad)

## Contacts

### Operational Security Team

* Email: [OperationalSecurityTeam@justice.gov.uk](mailto:OperationalSecurityTeam@justice.gov.uk)
* Slack: #security

### Dom1 - Technology Service Desk

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

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

### Digital & Technology - Digital Service Desk

* Email: [servicedesk@digital.justice.gov.uk](mailto:servicedesk@digital.justice.gov.uk)
* Slack: #digitalservicedesk

### Information Incident Reporting Line

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

During UK working hours, MoJ (but not HMPPS) staff should follow the process on the [Reporting a Security Incident](https://intranet.justice.gov.uk/guidance/security/report-a-security-incident/) page on the MoJ Intranet.

### MoJ Security

* Email: [security@Justice.gov.uk](mailto:security@Justice.gov.uk)

## Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [IT policy content](mailto:itpolicycontent@digital.justice.gov.uk).