Overseas Travel

Guide

Version: 1.3

Date: December 2021

Contents

[Official and private travel – guidance 3](#_Toc34815691)

[Procedures 3](#_Toc34815692)

[What to do if you hold National Security Clearance 3](#_Toc34815693)

[What to do if you want to take IT equipment on your trip 4](#_Toc34815694)

[International Roaming 4](#_Toc34815695)

[Travel preparations 4](#_Toc34815696)

[Competing visa applications 5](#_Toc34815697)

[Behaviour overseas 6](#_Toc34815698)

[Delegations involved in negotiations overseas 7](#_Toc34815699)

[Overseas connections 8](#_Toc34815700)

[Incidents overseas 8](#_Toc34815701)

[Dealing with gifts 8](#_Toc34815702)

[Other contact with foreign nationals 8](#_Toc34815703)

[After your return to the UK 9](#_Toc34815704)

[Visits to Foreign Missions within the UK 9](#_Toc34815705)

[Contacts 10](#_Toc34815706)

[Annex A – General advice 11](#_Toc34815707)

[Taking Official and Personal Electronic Equipment Overseas 11](#_Toc34815708)

[Use of Social Media Overseas 12](#_Toc34815709)

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

If you have any queries on the content of this document please contact [Security Team](mailto:Security@justice.gov.uk).

# Official and private travel – guidance

As a UK Government employee and because you work for an organisation that holds sensitive assets, you are more at risk from terrorists and hostile foreign states. These risks increase when overseas.

Some countries have an acute capability to steal information and they may seek to exploit opportunities associated with your overseas travel, regardless of your role or seniority and the threats from these countries can extend to environments beyond their national borders. Terrorist groups abroad have been known to attack foreigners and places where tourists may gather, such as hotels, transport systems, night-life areas and landmarks.

The nature and intensity of security threats is subject to change and varies from country to country. Staff should always consider Foreign and Commonwealth (FCO) travel advice for their destinations, even where they seem safe, and take with them details for the local Sovereign Missions (i.e. the local UK Embassy, Consulate or High Commission). Further guidance can be found at the FCO website [www.gov.uk/foreign-travel-advice](http://www.gov.uk/foreign-travel-advice).

## Procedures

Unless otherwise stated, these procedures are expected to be complied with fully.

**All staff must seek approval by submitting the** [Overseas Travel Form](https://intranet.justice.gov.uk/guidance/security/travelling-abroad-business-or-personal/) **from the** [Operational Security Team](mailto:OperationalSecurityTeam@justice.gov.uk) **if travelling to or through any of the following countries:**

Argentina, Armenia, Azerbaijan, Belarus, China (including Hong Kong, Macau and Tibet), Cuba, Egypt, Estonia, Georgia, India, Indonesia, Iran, Iraq, Israel (including Palestinian territories), Kazakhstan, Kyrgyzstan, Latvia, Lebanon, Libya, Lithuania, Moldova, the northern area of the Republic of Cyprus, North Korea, Pakistan, Russia, Saudi Arabia, Serbia, South Africa, South Korea, Syria, Taiwan, Tajikistan, Turkey, Turkmenistan, UAE, Ukraine, Uzbekistan, Vietnam.

### What to do if you hold National Security Clearance

Holding National Security clearance (SC, DV or Strap) increases the level of interest hostile foreign states have in members of staff.

All staff holding SC and DV clearances intending to travel to or through any of the countries above must complete the Overseas Travel Form at least 15 days in advance of the date of travel. Details of the purpose of the visit (including who you are meeting and where); the duration of the visit(s) and your accommodation arrangements must be provided.

Staff who are subject to a STRAP briefing must notify the STRAP team at [STRAPTeam@cluster2security.gov.uk](mailto:STRAPTeam@cluster2security.gov.uk) of their intended travel to any country (excluding countries in Western Europe, North America, Australia or New Zealand), and complete an Overseas Travel Form at least 20 working days in advance of travel or at the earliest opportunity.

Notification at short notice can place both the staff member and organisational assets at risk because there may be insufficient time to provide the appropriate help and guidance needed to manage the risk and you may not gain approval to travel.

SC, DV or STRAP cleared staff who fail to complete an Overseas Travel Form for their intended travel to or through countries listed above, when required, should be aware that this could affect suitability to hold a national security clearance and continue in their post.

### What to do if you want to take IT equipment on your trip

Any electronic device is at risk of compromise when you are travelling or visiting overseas. All portable technology, including laptops, smart phones and tablets can be tracked, intercepted, tampered with and potentially used as eavesdropping devices. Hostile foreign intelligence will seek to gain unauthorised access to information held both on official and personal IT systems and devices.

### International Roaming

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

**All staff must complete an Overseas Travel Form if taking any official portable or electronic devices to countries listed above.** This approval must be sought at least 15 working days before the date of travel. Annex A contains further guidance on taking electronic devices overseas.

## Travel preparations

As a Government employee, all staff must take active steps to manage the following risks in advance of all travel from the UK:

* Staff must not use diplomatic passports for private travel. Contact [Security Team](mailto:Security@justice.gov.uk) for advice if you have any diplomatic or official stamps in your passport.
* **All staff complete an Overseas Travel Form if intending to take any official work issued technology (or papers)** with them when travelling for private purposes. This includes, but is not limited to, security passes, documents and files, ID badges/warrants, electronic data, laptops, smart phones or tablets.
* Personal electronic devices contain a wealth of information about you and your personal contacts, including family, friends and your geolocation. The information can be used by Hostile State Intelligence to build a picture of you and your colleagues. You must assume personal devices will be compromised if taken to high threat environments such as the countries listed in the table above. The National Cyber Security Centre (NCSC) website details advice on mobile device security and the secure use of electronic devices at [www.ncsc.gov.uk](http://www.ncsc.gov.uk/).
* Further guidance is also available on [Accessing MoJ IT Systems from overseas](https://security-guidance.service.justice.gov.uk/accessing-moj-it-systems-from-overseas/#accessing-moj-it-systems-from-overseas) and Overseas Travel.
* Ensure you have the correct official documentation prior to travel, such as visas, landing cards, customs declarations and health certificates to avoid unwanted attention at the destination.
* Provide a detailed itinerary for your official travel to your Line Management as well as a personal point of contact in case of emergencies. Avoid making any reference to your travel details online or via any social media before or during travel.
* If you need to access sensitive information on an official trip it must be sent on a secure system (i.e. on a Government SECRET and above accredited system, such as ROSA) to the local UK Sovereign Mission where it can be arranged for you to view the material in a designated secure area. **ROSA laptops and mobile phones must never be taken overseas**.
* Staff have a duty to report if they have been approached by foreign interested parties, either in connection with their work or personally, whilst overseas or if any security incident has taken place, to [Security Team](mailto:Security@justice.gov.uk), no matter where these occur.
* Staff must obtain appropriate clearances for official travel via their Line Management and official travel arrangements should be made via an approved organisational booking process.

# Competing visa applications

Information given on a visa application may allow host countries to find travellers who may be of interest and this may potentially aid espionage efforts.

* Not every country will require a visa or details of employment, however, where such details are required, you should use generic terms and contact details and should avoid revealing the nature or specifics of their Government job title or place of work, for example Head of Security, the term ‘Senior Manager’ would suffice.
* You should not concoct stories or be dishonest; such stories can be difficult to support and arouse unnecessary suspicion.

Permanent staff:

* **Occupation:** use a general professional title, such as Manager or Administrator.
* **Contact details**: Building name, address (including post code).
* **Department**: Use name of relevant Government department.
* Staff should not share details about their Government department, directorate or unit
* If staff are asked for more information about the nature of their work, they should give a routine element of their work, such as policy work or admin work. Staff should avoid using terms such as ‘security’ or ‘defence’.
* If needed, letters should be on official headed paper of their relevant Government department.

Permanent staff (ALBs):

* **Occupation**: use ‘Government service’.
* **Contact details**: ALB staff should give the address for their organisation’s headquarters and only offer the name of their organisation if specifically asked.
* If ALB staff are asked for more information about the nature of their work, they should give a routine element of their work, such as policy work or admin work, and avoid using terms such as ‘security’ or ‘defence.’

Temporary or contracted staff:

* **Occupation**: use a general professional title. Temporary or contracted staff should make no reference of their work for their Government department.
* **Contact details**: give the company’s business address.

# Behaviour overseas

You should always consider that your behaviour could bring you to the attention of state and law enforcement authorities, as well as, foreign intelligence services and this can be serious. As a Government employee, you should abide by the following to minimise the risk of compromise:

* Be discreet when talking about your work. Sensitive discussions should always take place in designated secure areas in UK Sovereign Missions.
* In countries of concern, you should assume that the contact details (telephone, email etc) of anyone you contact will be collected and may be used for future intelligence gathering. Similarly, any personal details you may have given to contacts, such as home address, telephone number, email address, could also be passed onto the intelligence services.
* Check the identity of those you are meeting and be wary of people who show unusual or heightened levels of interest in your work or the MoJ.
* Do not offer business advice for any purposes which could imply that normal procedures could be bypassed.
* Do not enter an officially prohibited zone without permission from a recognised authority.
* Avoid areas of civil war, unrest or protest.
* Do not make controversial statements in public, this will include, but is not limited to comments on any country’s political situation or leader(s) and its religion(s).
* Be aware of and abide by local laws.
* Be alert to compromising situations and be wary of being coerced into activity during which your judgement might be impaired (e.g. drinking, drug taking, gambling, flirtatious liaisons). In some countries, some sexual practices may be illegal and may result in arrest and/or attempts to blackmail by the local security and intelligence services. Many prostitutes are employed by the local security service to report any dealings with Western visitors.
* Avoid carrying official paperwork, wherever possible, when on business.
* Exercise caution on where and how you use camera and recording equipment. Filming and photography should be restricted to normal tourist attractions. In some countries, using a camera in poor or prohibited areas or taking photographs of aircraft or some installations can lead to accusations of espionage. When in doubt about taking photographs or footage, local permission should be sought from a recognised authority.
* Hotel safes should not be trusted for storing sensitive or personal information or electronic devices, as these may be defeated by capable adversaries.

## Delegations involved in negotiations overseas

Members of staff involved in any overseas negotiations are likely to be of interest to a range of adversaries, seeking to undermine or influence the UK Government’s negotiating position. Adversaries will be interested in key staff and organisations developing the negotiating position and their roles to support any targeting of, and access to, the key decision maker in any negotiation. To minimise the risk of compromise and make it harder for adversaries to identify and target staff, you should:

* Avoid compiling delegate personal contact details onto one place/document and do not allow distribution of these contact details beyond those who need to know.
* Keep baggage, possessions and electronic devices secure and do not hand them over to anyone or leave unattended in hotel rooms or safes. Check your possessions for evidence of tampering and report any strange behaviour of electronic devices to security.
* Make use of official vehicles for travel wherever possible.
* Avoid holding sensitive conversations in areas where you may be overheard.
* Avoid travelling as a large delegation and staying at same hotel if return visits are required.
* Protect electronic, hard copy and notes relating to the negotiations, by keeping them in sealed opaque envelopes; particularly sensitive information should remain with the UK Sovereign Mission.
* Follow the guidance and policy outlined in the Behaviour overseas section of this document.

## Overseas connections

Staff and/or their family members who are of dual-nationality or have changed their nationality, could be at risk if their original country does not recognise changed or dual nationality. This can cause the foreign intelligence service to exploit family connections and/or perceived patriotism. Staff should be aware that anyone they meet could be later be interviewed by the country’s intelligence service and questioned about them, as such, contact or liaisons should be kept to a minimum. Further guidance on this matter can be obtained from [Security Team](mailto:Security@justice.gov.uk).

## Incidents overseas

Staff should report any of the following occurrences to [Security Team](mailto:Security@justice.gov.uk) if:

* Arrested or detained.
* Involved in a security incident.
* Involved in an unusual incident or something out of the ordinary occurred (no matter how trivial).
* Approached (in person or online via email or social media) with an unofficial request for help or information to circumvent official procedures.

Where staff encounter problems, or feel that they may have been compromised, they should:

* Never give any undertaking to ‘co-operate’ in exchange for charges being dropped.
* Never admit to wrong doing, particularly by signing a document, except on the advice from an official of a British Mission.
* Report the situation as fully as possible to the local British Mission at the earliest opportunity.
* Make a written report to your Home Department’s Security Unit on your return to work, including full details of the issue.

## Dealing with gifts

Hosts may offer gifts and hospitality to you, but you should be cautious. Any gifts or offers of hospitality provided by overseas, delegation or Foreign Mission hosts can be used to develop a relationship with you to facilitate access to your contacts or information and gifts may contain covert monitoring equipment or malware which can be used to compromise IT systems. You must not use any gifts including, phones, tablets, chargers, USB, mobile battery packs that are given to you and these must be handed in to [Security Team](mailto:Security@justice.gov.uk) on your return to the UK.

## Other contact with foreign nationals

Staff should be alert to the potential danger of revealing detailed information about their employment or security clearance in conversation, correspondence, interviews, publications, questionnaires, electronically or via the internet, as well as via training courses, trade fairs, conferences, lectures, exhibitions and through subscription to specialist journals.

These actions may have the effect of making staff the potential target of a foreign intelligence service or a terrorist organisation or may leave the staff member liable to pressure to reveal information or to influence the outcome of an application.

Staff in regular and close contact with nationals of countries listed in the Procedures section of this document (both in an official or non-official capacity, and irrespective of whether they are based in the UK or abroad) should consult [Security Team](mailto:Security@justice.gov.uk) for advice.

[Security Team](mailto:Security@justice.gov.uk) should be consulted if contacts, from any country, seem unusually interested in your work or in any other way to raise cause for concern from a security point of view.

# After your return to the UK

Information may be gleaned about staff during their overseas trips, which can be used to make contact once they have returned. This may be remotely, e.g., a spear-phishing email attack (targeted attempt to steal sensitive information), or staff may be subject to an approach after your trip, either in person or online (i.e. online activity such as unknown social media requests via LinkedIn, Twitter, Facebook, etc.).

On returning to the UK, you should:

* Be alert to any strange behaviour of electronic devices and suspicious activity relating to online accounts, particularly social media.
* Be extra vigilant for emails that have links or attachments. If you do click on a link or open an attachment that you think is malicious, inform the Technology Service Desk

( 0800 917 5148.

* Contact [Security Team](mailto:Security@justice.gov.uk) if anyone approaches you after your trip, either in person or online.
* Staff should change their passwords for electronic devices and accounts that were used overseas.
* Submit any gifts you have received to [Security Team](mailto:Security@justice.gov.uk).

# Visits to Foreign Missions within the UK

The risk to information, assets and staff is greater in a foreign mission’s own environment. [Security Team](mailto:Security@justice.gov.uk) must be consulted for approval and advice and staff should send their request for advice **at least a week in advance** of the visit.

Where approval is given, staff should be aware of the risks associated with such visits and apply the following protective security measures:

* Visits should be made by at least two officers.
* Sensitive information should not be taken into or discussed within Foreign Mission buildings (including into meetings).
* Official work issued portable or electronic devices (such as mobile phones and laptops) should not be taken to such meetings.
* Apply the policy guidance and principles outlined in the Behaviour overseas section of this document.
* Offers of hospitality or gifts should be treated with caution, see the Dealing with gifts section of this document. If staff have received official or unofficial invitations to events or dinners held by the Mission or any of its staff, the prior approval of [Security Team](mailto:Security@justice.gov.uk) must be sought before attending such events. In most circumstances, where the visit is not business critical, officers will be advised not to attend.

Any requests or approaches by foreign officials that are not related to what has been agreed to discuss or would be considered inappropriate or have been made post visit should be resisted and must be reported at once to [MoJ Group Security](mailto:mojgroupsecurity@justice.gov.uk).

# Contacts

|  |  |
| --- | --- |
| For **personal advice on travelling overseas** and for notification of proposed travel with foreign nationals. | [Security Team](mailto:Security@justice.gov.uk)  (Security@justice.gov.uk) |
| For advice on **taking any official portable or electronic devices overseas.** | [Operational Security Team](mailto:OperationalSecurityTeam@justice.gov.uk)  (OperationalSecurityTeam@justice.gov.uk) |
| For **personnel and physical security advice.** | [Group Security Team](mailto:mojgroupsecurity@justice.gov.uk)  (mojgroupsecurity@justice.gov.uk) |
| For advice if you **clicked on a link or opened an attachment** that you think **is malicious**. | Technology Service Desk  Tel: 0800 917 5148 |

# Annex A – General advice

## Taking Official and Personal Electronic Equipment Overseas

**All staff must seek approval to take any official portable or electronic devices to countries listed in the table in the Procedures section of this document**. Approval must be sought from the [Operational Security Team](mailto:OperationalSecurityTeam@justice.gov.uk) by completing the [Overseas Travel Form](https://intranet.justice.gov.uk/guidance/security/travelling-abroad-business-or-personal/). This approval must be sought at least 15 working days before the date of travel. This annex contains further guidance on taking electronic devices overseas.

You must review the risks of any data for information being carried (both printed and electronic) when travelling and you are advised to take only data needed for your overseas trip. This applies to officially issued, as well as, personal portable/mobile devices. You may be prevented from taking some or all equipment to certain destinations.

* In host countries it may be assumed that their foreign intelligence service will have a presence at the borders and customs, major hotel and conference venues and in local or national telecoms centres and organisations. The threats from these include:
* interception
* electronic attack
* tampering and theft of portable/mobile devices.

A high priority is placed on targeting HMG communications overseas and British Officials.

* Some Foreign Governments have legislation in place that restricts the use of or taking of devices across their borders, and if it is deemed to be in their national interest, permits them to demand that devices are decrypted and/or retained, which could pose a threat to personal security.

If you are authorised to take official electronic equipment, you should be aware that:

* **Immediately when a device is switched on it is vulnerable to both a communications interception, including emails and telephone.**
* Do not connect to untrusted Wi-Fi networks that either have no authentication method and/or you do not know who is providing the Wi-Fi network. Wi-Fi and plugged laptop connection points may be monitored.
* Do not place your device in checked baggage;
* Portable/mobile devices are an attractive target to thieves and this presents a risk to sensitive data being extracted; keep your devices in view at all times. Laptop encryption is rendered useless if the user credentials and passwords are kept with the device.
* Be aware of your working environment; unfamiliarity of surroundings and the associated risks provides a greater opportunity to engineer or exploit vulnerabilities.
* Portable/mobile devices should not be left unattended to reduce the risk of tampering or theft. Portable IT equipment is often targeted by thieves and it is advisable to keep them out of sight or carry them in plain unmarked bags wherever possible.
* Do not leave mobile devices unattended in hotel rooms, or hand them over at any point, they may have been subjected to modification before being returned.
* The necessary levels of physical security may not be present in non-government buildings, hotel or conference facilities and it is important not be lulled into a false sense of security by the limited physical controls that may exist. Do not rely on hotel security procedures (e.g. safes) to prevent unauthorised access.
* Users should be vigilant about people eavesdropping or observing the screen over their shoulder (‘shoulder surfers’).
* Any organisation or individual that can gain access to the telephone network can intercept calls, potentially at several points along its route. Overseas communications via cable offer no inherent protection.
* Think before posting any comments on social media before or regarding your trip. This may highlight areas of interest to people who could pose a threat in the destination country.

## Use of Social Media Overseas

* Social media platforms on work devices should not be used to convey official information.
* It is important to remember that when posting on social media platforms in a personal capacity you may still easily be identified by others as working for the Government even if you don't state it.
* Treat all voice and text messages as potentially compromised; end to end encryption does not mean that communications such as WhatsApp are secure.
* Do not switch location sharing on, unless necessary in a crisis.
* Dating apps always require geolocation services, which remain running when the user is no longer in the app, this can give unauthorised people access to your location and movements as well as personal information. If you are no longer using an app delete it and any associated data from your phone.