#Taking equipment overseas

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

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

##General guidance

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

##Keeping safe whilst conducting sensitive work overseas

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

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

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

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

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

* Try to establish your official status and good faith from the outset.
* Remain calm and polite at all times.
* Carry the names and telephone numbers of a relevant departmental contact and invite the official(s) to contact them to confirm that you are who you claim to be.
* If the official continues to insist on the user inputting his/her password, repeat the 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](#contacts) and report the device as potentially compromised.

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

##Contacts

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

**If unsure, contact your Line Manager.**

##General enquiries, including theft and loss

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

* Tel: 0800 917 5148
* [MoJ Service Portal](https://mojprod.service-now.com/moj_sp)

**Note:** The previous itservicedesk@justice.gov.uk and servicedesk@digital.justice.gov.uk email addresses are no longer being monitored.

**Note:** Use of the Digital & Technology Digital Service Desk Slack channel (#digitalservicedesk) is being withdrawn, and should be avoided.

**HMPPS Information & security:**

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

##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).