# Guidance for Business Travel to High Risk Countries

# Introduction

The benefits of travelling to overseas countries for business are wide and varied, and are an integral part of University business. However, there are some locations where the risks of doing so are increased. These risks cover different aspects such as health, regulatory, security or natural events and the likelihood and consequences of them will vary from location to location. This advice document covers the potential increased information security risks associated with overseas travel, focusing on those countries where this specific risk is deemed to be ‘High’.

Travellers to high[[1]](#footnote-1) risk countries should be prepared for a different experience due to local customs and laws. For example, people visiting China have reported a range of security issues such as restricted access to popular services (eg internet based email services, Wikipedia, social media sites); government monitoring of communication services such as Skype; unreliable and insecure Wi-Fi connections and hotel staff or government officials accessing electronic devices left in hotel rooms.

# Information Security Advice

The following advice applies to University colleagues who plan to travel to high risk countries with University provided equipment or with personal devices (phones, laptops, tablets etc) used to access University services or process University data. It is also good practice for those using personal devices for their own activities. If you are unsure how to carry out any of these points, you should check your device ‘Help’ pages to confirm how to do them.

**Before you Travel:**

Ensure you include information security risks in your risk assessment ([Business travel | The University of Edinburgh](https://www.ed.ac.uk/staff/business-travel))

Discuss your travel arrangements with your local IT support team to make sure you can continue to work whilst away. Test the equipment, applications and procedures you plan to use well in advance of travelling

Ensure that you are using strong passwords for all your devices (for guidance see <https://www.ed.ac.uk/infosec/how-to-protect/lock-your-devices/passwords>)

Back up all your University data to University managed storage (for guidance see <https://www.ed.ac.uk/infosec/how-to-protect/backups> )

Ensure you set up multi factor authentication wherever it is an option, and check you have configured multiple authentication methods to include some that are not reliant on a mobile phone in case of loss or if you are not taking that mobile phone with you. For guidance see [Choosing an authentication method](https://www.ed.ac.uk/information-services/computing/computing-infrastructure/authentication-authorisation/multi-factor-authentication/register/guide-to-choosing-an-authentication-method) and [MFA and travel](https://www.ed.ac.uk/information-services/computing/computing-infrastructure/authentication-authorisation/multi-factor-authentication/mfa-and-travel)

Identify all passphrases/passwords saved on your devices and remove any that are not needed whilst you are away. Consider using a password manager to securely store any passwords you do need – examples of available managers are listed on the Information Security website (<https://www.ed.ac.uk/infosec/how-to-protect/lock-your-devices/passwords>)

Specifically log out of any online services you do not plan to use while travelling, particularly any service which does not normally require a login if opened in your usual browser

Clear local browser and downloaded cache/history files

Disable all unnecessary services on your devices, including USB ports, WiFi and Bluetooth, if possible.

If you will need to use WiFi then ensure that you know how to enable and disable WiFi on the specific devices you are taking with youEnsure that all devices are fully patched and up to date

Ensure that you have enabled encryption where this is available for your device

If you need to take University data with you, ensure this is the minimum needed for the specific trip and remove any data that is not needed, particularly any commercially sensitive data or data containing personal identifiers

Consider setting up specific folders in OneDrive and setting controls to allow access for individuals with whom you may need to share information when away. Limit what information is stored in these folders

Ensure that you can uniquely identify all your devices (stickers, specific marks etc) to prevent any attempt to substitute them

Check that your country of destination allows encrypted devices to be taken in and out (for further details see <http://www.cryptolaw.org/> and <https://www.gp-digital.org/world-map-of-encryption/> )

**While Travelling:**

Keep all documents, mobile devices and chargers with you at all times and do not leave unattended in hotels etc. Where possible, carry these in hand luggage whilst travelling

Equipment sold to travellers in a high-risk country, such as chargers and other electronic devices, may be compromised and should not be connected to University equipment or used for University purposes. Consider taking a spare charger and appropriate adapter plug

Think twice about all ‘normal’ actions: use common sense and a higher degree of suspicion to consider whether someone may be attempting to steal or subvert your information

Only enter University usernames and passwords into your own device or one provided by the University of Edinburgh

Only use your own chargers, never one that you have borrowed. Similarly, do not use public charging points in café’s, airports etc

Disable microphones and cameras in laptops (ensure that you know how to do this for the specific device you are taking with you as this may be different for each type of laptop)

Do not use or accept removable media such as USB sticks, external hard drives or anything that can plug into your device

Use your limited access OneDrive folder to share information when away, to avoid the need for use of removable media. Grant additional access to individuals as-needed and remove data after it has been shared, after scanning for viruses

Be aware of your surroundings if holding sensitive conversations – assume that your calls and discussions are being monitored

Never lend you devices to anyone who is not a University of Edinburgh employee

Keep WiFi disabled whenever you are not actively connecting to a WiFi network.

If connecting to public WiFi you are asked for an email address do not use your University email: use ‘traveller@ed.ac.uk’ instead (this account has been created specifically for this scenario and cannot be used for anything else). If you are asked to set a password for the WiFi then ensure that you do not use the same password as for your University account or any other service; it is best to use a random password. If the WiFi provider seeks to download anything to your device or says it has sent a link to the address you provided then do not use it as it is likely that it is trying to download malware. Disconnect and delete it from your networks.

Use VPN’s to access University services and sensitive data that is not publicly available

**When you get home**

If your devices or chargers have been out of your possession during the trip, even briefly, then consider them to be compromised and arrange for any University supplied device to be rebuilt, with data restored from a pre-trip source, and any chargers disposed of and replaced. Consider doing the same for personal devices

From a device that was NOT with you, reset all passwords/passphrases that you may have used whilst away (you should do this for University accounts and for any personal accounts you accessed)

The following advice also applies:

**Good**

* Only travel with the minimum information you need
* Use encryption, but be prepared to decrypt devices or files at border control points if asked to by local officials. This may involve you unlocking your device or opening the file and showing content to the official. If possible, you should remain with your device once unlocked (it is recognised that this may not always be possible)
* Make sure mobile devices are secured, data is backed up, software is up to date and unneeded data removed

**Better (in addition to Good)**

* Leave current devices behind and take a newly built encrypted device with you
* Use a new mobile phone that will be disposed after your trip or only used on subsequent trips. It should not be used for any University business, and no University data or University usernames or passwords should be accessed, stored or used on this device. Additionally, it should not be used as an MFA authentication method. Either get this before you go or when you get there.
* If you intend to use the device on subsequent trips then you should power off and not use the device outside of the intended country.
* Use VPN to connect to University services
* Make use of secure remote access technology if you need to access data

**Best (in addition/instead of Better)**

* Leave usual devices behind and take a newly built laptop with no encryption’ (Clean laptop service available ([Before you go | Information Security (ed.ac.uk)](https://infosec.ed.ac.uk/information-protection-policies/guidance-how-to-conform-with-policy/remote-working/working-while-travelling/before-you-go)) locked USB ports and without a local administrator account
* Do not store any University data on any device you take with you – use OneDrive or University shared drives and access via VPN
* Do not use mobile devices that allow storage or connection to removable devices such as USB – make sure these are disabled before you travel
* Only connect to University services via VPN. If this is temporarily unavailable, wait to connect. If the VPN Is not available and you need to communicate with colleagues, ensure that you do not include any sensitive information in your communications
* Do not check emails or remotely access any other services that store University data via insecure connections – always use a VPN
* If you can’t be without a mobile phone (best option for shorter, one-off trips), obtain one locally and dispose of it after the journey. Absolutely no University data or University usernames and passwords should be accessed, stored or used on this device. It should not be used as an MFA authentication method. Never discuss any sensitive University business on a call.

# Additional Information

Additional information is available from the following sources:

* University policies and guidance relating to Business Travel:

[Business travel | The University of Edinburgh](https://www.ed.ac.uk/staff/business-travel)

* Travel advice and general guidance is available from the UK Foreign and Commonwealth Office. Travellers can check their website prior to, or during, overseas travel:

<https://www.gov.uk/foreign-travel-advice>

Note that colleagues from overseas should check travel advice provided by their own government as country risk profiles might be different from that supplied by UK government.

1. Countries presenting a ‘high’ information security risk include: China, Iran, North Korea and Russia. A list of high risk countries is available on the Information Security website at [Before you go | Information Security (ed.ac.uk)](https://infosec.ed.ac.uk/information-protection-policies/guidance-how-to-conform-with-policy/remote-working/working-while-travelling/before-you-go) [↑](#footnote-ref-1)