Cyber Security Guidance: Travel to 'High' Risk Countries

Introduction

These instructions are for Brunel University staff, and researchers who are working from a country presenting a 'high' information security risk where there is an increased risk of data and identity theft.

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.

Travellers to high[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 (e.g. internet-based email services, social media sites); government monitoring of communication services; 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 working on behalf of the University from 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.

Before you Travel:

1. **Discuss your travel arrangements with the IT Service Desk Team** to ensure that your university account will be accessible from the region you are travelling to, and that you can continue to work whilst you are away.

2. **Ensure that you are using strong passwords for all your devices**. Strong passwords are the first line of defence for your accounts. They protect your email and your data. The longer the password is the harder it is for it to be 'guessed' or brute forced. (for guidance see https://www.staff.brunel.ac.uk/directorates/information-services/passwords-cyber-security)

3. **Back up all your university data to your university managed storage areas.** Either a dedicated research storage area or Brunel M365 SharePoint or OneDrive cloud storage.

[1] Countries presenting a 'high' information security risk include: China, Iran, North Korea, Russia, Brazil & Turkey.

4. **Assess whether your devices contain any work, data, or technology that may be subject to export control legislation.** This includes laptops, phones and other electronic devices – **Important:** Exporting controlled items without the appropriate licence is a criminal offence. See Appendix A for guidance on export control considerations.

5. **Set-up multi factor authentication on all your accounts (incl. personal accounts) where it is available.**

6. **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 will need while you're away.

7. **Download cache/history files and clear browser history from your device.**

8. **Disable all unnecessary services on your device,** including USB ports, Wi-Fi and Bluetooth if possible.

9. **Ensure that all devices are fully patched and up to date.** This includes the basic operating systems, anti-virus protection, applications, and device firmware such as the BIOS. It's always advisable to keep your device up to date because this reduces the number of ways it might be vulnerable to attack. **It's best to do any updates in an environment you trust. So, make sure all available updates are applied before you travel.**

10. **Ensure that you have enabled encryption[2] where this is available for your device and if allowed by your country of destination.** 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).

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

12. **If you need to take University data with you, ensure this is the minimum needed for the specific trip.** Ensure that files are saved to your Brunel M365 SharePoint or OneDrive cloud storage area.

13. **Do not save any files locally on your device.** However, if you anticipate that you won't have access to the internet or you are traveling to Iran or North Korea where access to most web-based applications is restricted, you may save critically necessary files with a classification status of *Protect* but it must be encrypted. Know their file names and description of contents in the event that your device is stolen and where possible ensure that they are backed up to your Brunel M365

[2] Depending on where you are in the world, the legal status of encryption varies significantly. Further information can be found here - https://www.gp-digital.org/world-map-of-encryption/

cloud storage area. **Note: under no circumstances should University Confidential data be saved locally on a device.**

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

While travelling:

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

2. **If your device goes missing or is confiscated, contact the Brunel IT Service Desk as soon as possible**. If it is returned, assume it is compromised; do not turn it on or conduct any business on it for the remainder of your trip.

3. **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 information.

4. **Be aware of your surroundings if holding sensitive conversations.** Assume that your calls and discussions are being monitored.

5. **Never lend your devices to anyone (other than known University colleagues).**

6. **Only enter your university username and password on your university provided device or personal device. Do not use your university account credentials on public devices, for example in internet cafes, hotels, airports etc.**

7. **Only use your own charger, never one that has been borrowed.** Similarly, don't use public charging points in café's, airports etc.

8. **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 depending on the model).

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

10. **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.

11. **Do not connect to any public Wi-Fi hotspots using your university username and password.**

Returning from your Trip

1. **If your device(s) or charger(s) have been out of your possession during your trip, consider them to be compromised.** Contact the IT Service Desk to arrange for your university supplied device to be rebuilt, with data restored from a pre-trip source. Consider doing the same for personal devices.

2. **From a device that you did NOT take on your trip, 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).

Additional Information

- University policies and guidance relating to Travel Safety: https://students.brunel.ac.uk/documents/Policies/travel-safety-business-and-study-2023-2026.pdf

- 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.

- University Bring Your Own Device Policy: https://students.brunel.ac.uk/documents/Policies/pol-byod-policy-v1.0.pdf

APPENDIX A

Export Control Considerations

Before travelling abroad, assess whether your devices contain any work, data, or technology that may be subject to export control legislation. This includes laptops, phones and other electronic devices.

UK Export Control Overview
UK strategic export controls focus on high-risk activities such as applied research. These controls may apply if you:

- Collaborate with overseas colleagues on research projects
- Take research materials or technology abroad
- Export technology or data

Important: Exporting controlled items without the appropriate licence is a criminal offence. Penalties may include:

- Revocation of licences
- Seizure of items
- Financial penalties
- Imprisonment (up to 10 years)

Travelling Abroad with Controlled Items

1. If You Have an Export Licence

- Notify RSDO by emailing trustedresearch@brunel.ac.uk before travelling on university business with controlled items.
- You may use your electronic devices as normal, including accessing Outlook and downloading attachments.
- You are permitted to carry out all controlled work as specified in your export control licence.

2. If You Do Not Have an Export Licence

- Do **not** take any electronic devices containing controlled data, research, or technology abroad.
- If you need a laptop for travel:
    - Request a blank device from IT Service Desk for non-controlled data
    - Or remove all controlled information from your current device before travel
- Use **Webmail** (not Outlook) to access emails while abroad.
    - Do **not** open attachments suspected to contain controlled data.
- Do **not** access controlled information via university shared drives or servers while overseas.

If you are unsure whether your work falls under the UK Strategic Export Control List, please contact the Trusted Research team at trusted.research@brunel.ac.uk to request an Export Control assessment.