INTERNATIONAL TRAVEL WITH PORTABLE DATA STORAGE DEVICES AND ENCRYPTED LAPTOPS

1 Risks

Mobile technology provides the opportunity to access your work worldwide. Data can be held on a variety of portable storage devices such as laptops, USB sticks, mobile phones, iPads, iPods and removable hard drives. However, the likelihood of portable storage devices being lost or stolen is high, particularly when travelling, and you need to take steps to ensure that data is not irrecoverably lost and confidential data does not fall into the wrong hands.

2 Do's and Don'ts

2.1 Plan ahead.

2.2 Ensure that all data on portable devices is backed-up on University servers before you leave eg OneDrive, SharePoint Online, p drive, shared drive.

2.3 Keep to a minimum any data that you need to take with you and avoid taking overseas any personal data, confidential information or data which is subject to contractual constraints, regardless of the country you are visiting - if it is essential that you have access to such data, you should use the secure web access to the University's OneDrive or SharePoint Online, or use Outlook.com (the web version of Outlook), as VPN connections may not be permitted in all countries.

2.4 No personal data (eg related to staff, students, research participants etc) may be taken outside the EEA without consultation with the Information Governance Office.

2.5 If challenged at border controls, you should ensure that the device has power and any usernames or passwords are readily available to assist in unlocking the device or accessing the data.

2.6 Please read Section 3 below as encrypted devices may not be allowed in some countries unless you obtain appropriate import licences. As it is University policy that all laptops must be encrypted, you must arrange for your laptop to be decrypted or request the loan of a new or clean laptop from IT Services.

2.7 Remember that the laws of a country can change at any time. Therefore, before travelling internationally, it is important to ensure that you have the most up-to-date information about travelling with encrypted data or devices.

3 Import and export controls related to encryption

Whilst many countries allow visitors to bring portable devices through border controls unchallenged, some countries try to restrict the use of encryption and require the possession of appropriate import/export licences. Attempting to take encrypted data or devices to these countries without obtaining licences may result in the device being confiscated or other penalties including imprisonment.

Directorate of Compliance and Risk
February 2022

3.1 UK and US export controls

UK and US export controls apply to export by either physical or electronic means from the UK and US. If a product is restricted, then a licence to export that product is required.

As long as the encryption software used is a mass market product that is freely available to the public, its functionality cannot be changed by a user and it can be installed without substantial support by the supplier, it will not be necessary to obtain a UK export licence for such software. Accordingly, provided that the encryption software that you use fits these criteria, you can freely travel from the UK with encrypted data or devices, without the need to seek export permission for that encryption software (but you still require a licence if you travel with other controlled information in your encrypted device). Alternatively, you can travel with a blank device which you can request from IT services. The University's recommended encryption software does not need an export licence.

However, if the encryption software that you use does not fit the criteria set out above, it is likely that you will need to obtain a Cryptography Open General Export Licence (OGEL). Contact the University Export Control Compliance (ECC) Team for assistance. Further details can be found at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/977130/Open-General-Export-Licence-Cryptographic-Development-from-December-2019.pdf

If the encryption software that you use is originated in the USA, the US export legislation may apply as well. Contact the University Export Control Compliance (ECC) Team for assistance.

3.2 Countries which you can freely enter with encrypted data or devices

While "personal use exemptions" which allow individuals to enter countries with encrypted data or devices without the need for a licence, it is better to check with the country you're travelling to beforehand https://www.comparitech.com/blog/vpn-privacy/encryption-laws/.

Remember, even though you may not need a licence to take encrypted data or devices into a country, upon entry, you may still be asked to disclose the data, so it's safest not to take personal or very sensitive data with you.

3.3 Countries for which you need permission to enter with encrypted data or devices

If a country requires an import licence, they are usually obtained by applying to the government of the country in question. The following website provides the contact details for some countries: https://www.wassenaar.org/participating-states/

Be aware, that even with a licence, your laptop may still be searched and you may be asked to decrypt it.