Travelling abroad with technology

<table>
<thead>
<tr>
<th>Author</th>
<th>P Green</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved by</td>
<td>P Green / B Kennedy</td>
</tr>
<tr>
<td>Approval date(s)</td>
<td>P Green / B Kennedy</td>
</tr>
<tr>
<td>Review date</td>
<td>Last: May 2018 / Next: May 2019</td>
</tr>
<tr>
<td>Version</td>
<td>1.1</td>
</tr>
<tr>
<td>Document type</td>
<td>Policy</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>NA</td>
</tr>
</tbody>
</table>
Introduction

If you are required to travel abroad on University Business, please also see the pages here;

https://www.st-andrews.ac.uk/administration/planning/insurance/university-travel/

Before you travel, remember all University-owned laptops and mobile devices must be encrypted. The University uses encryption to protect data should the device be lost or stolen. In this case, this means data which the University classes as;

Confidential
Strictly Confidential

Please see;

https://www.st-andrews.ac.uk/itsupport/security/classification/

For more details.

However, in some countries you need permission before you can bring in an encrypted laptop or other device. In other countries, encryption is banned. In practice, this means that if you are unable to use encryption within a country, then that device is not suitable for storing strictly / confidential information.

Further to this, ITS has assigned “risk” based categories to countries to identify if encryption can be used and the perceived risk of using an encrypted laptop within a country. The categories are summarised as;

Green: You can take in encrypted devices
Amber: You will need to request a licence to import encrypted devices
Red: ITS strongly advise that you do not take in any devices which are encrypted

Country list

Green countries
members of the Waasenaar agreement that recognise personal use [1]

• Argentina
• Australia
• Austria
• Belgium
• Bulgaria
• Canada
• Croatia
• Czech Republic
• Denmark
• Estonia
• Finland
• France
• Germany
• Greece
• Hungary
• Ireland
• Italy
• Japan
• Latvia
• Lithuania
• Luxembourg
• Malta
• Mexico
• Netherlands
• New Zealand
• Norway
• Poland
• Portugal
• Republic of Korea
• Romania
• Slovakia
• Slovenia
• South Africa
• Spain
• Sweden
• Switzerland
• Turkey
• United Kingdom

**Amber Countries**

These countries require an import licence for taking an encrypted device

If a country is not included in the list of Green Countries, it is likely that an individual travelling to such country with an encrypted laptop will need permission, usually an import licence, to enter the country with the laptop (the traveller must request this). Such import licences are usually obtained by applying to the government of the country in question. Be aware, though, that even with a licence, your laptop may still be searched, and you may be asked to un-encrypt it. Please check the list of RED countries before assuming a country has an Amber rating.

If you would like a loan laptop and phone / tablet which aren’t encrypted, please let ITS know and they will provide you with loan devices for the duration of your travel.
**Red Countries**

Certain countries have been listed as being “high risk”. For these countries either, encryption needs a licence and there is a high level of risk associated with taking in an encrypted laptop or encryption is embargoed and it is illegal to take encrypted devices into the country.

- Russia
- China
- North Korea
- Cuba
- Iran
- Sudan
- Syria

For countries which are marked as RED please let ITS know that you are travelling to the country and they will provide you with a loan laptop and phone. These will be basic devices and are not suitable for storing strictly / confidential data. When you return to the UK, please bring the devices back to ITS.

You will not be able to use the VPN service and the loan phone will not be a smart device and won’t have a passcode installed.

Please access email and files through outlook web access and MS One Drive only

When you return, please ensure you change your passwords. Return the loan devices to ITS.

**Loss of devices**

Before you travel, please familiarise yourself with the ITS process on lost or stolen devices. You will be required to follow this advice if you find your devices lost or stolen;

https://www.st-andrews.ac.uk/itsupport/mobile/smartphones/iphone/hintsandtips/lostorstolen/

**Other precautions**

To protect our data, we also advise the following;

- Do not use internet cafes for accessing resources that require a username and password
- Do not use USB devices that are given as gifts
- Do not connect to free wireless networks
- Change passwords for services you accessed whilst in Amber or Red countries when you return to the UK
Notes
Please assume that in any country, the local authorities can request the decryption keys and you should comply with any official requests.

If you receive information, when in country, that is classed as Strictly / Confidential, then this is permitted to be stored on an unencrypted laptop. The information should be transferred to an encrypted device on return to the UK [2]