Travelling abroad with your University laptop

Your University laptop is encrypted so that information stored on it cannot be accessed if it is lost or stolen. It also contains special hardware which assists with this encryption. As well as protecting your information, this also ensures that you are complying with University Information Security policy.

In some countries the use of encryption (or possession of encryption hardware, even if unused) is either controlled or illegal.

In some cases you may need to obtain permission (an import licence) to take an IT Services managed laptop (or equivalent) with you; in others you should not take your laptop with you at all.

- What you need to consider
- Countries with known controls or issues
- Further advice

Is my University laptop encrypted?

If you have a standard IT Services managed laptop which has been encrypted, you will be prompted for a PIN (personal identification number) when you first switch it on. These laptops contain hardware which manages this encryption in a convenient and secure way.

If you are using a laptop which does not prompt you for a PIN in this way or are unsure about whether your laptop is encrypted, contact the IT Service Desk who will help you to determine this.

What about USB memory sticks / external hard drives?

USB memory sticks and external hard drives aren’t encrypted by default. However you may have purchased encrypted USB memory sticks or hard drives through IT Services. The same issues which affect encryption and encryption hardware on laptops will apply to those devices as well.

Again, if you are unsure, you should contact the IT Service Desk who will help you to determine this.
What you need to consider

There are four major issues you need to consider if you are planning to take your laptop with you when travelling abroad:

1. **Illegal**: It may be illegal to use encryption or take encryption hardware into a country.
2. **Import licence**: You may need an import licence to use encryption or take encryption hardware into a country.
3. **Information disclosure**: You may be required to disclose encryption key(s) to local authorities (e.g. customs officials) to enable them to access encrypted information.
4. **Tampering**: In some countries, attempts may be made to tamper with your laptop e.g. to install key-logging hardware or software, putting your information at risk.

The University does not want to put staff or students in a position where they are breaking the law when travelling abroad. You **must** consider these issues before travelling and think about whether you are putting yourself or your information at unacceptable risk as a result of having (or failing) to comply with the law in other countries.

Where encryption or possession of encryption hardware is illegal

In countries where the use of encryption or the possession of encryption hardware is illegal, you must not take an IT Services managed laptop, any other encrypted laptop or encrypted USB memory stick or hard drive with you.

If you do, then you may:

- be prevented from entering the country you are travelling to, disrupting your work
- have your equipment confiscated (and possibly not returned) resulting in both inconvenience to you and financial cost to the University
- in extreme cases, face detention or arrest.

If you are travelling to a country where this is the case and it is critical that you have a laptop for work purposes when abroad, you should contact the IT Service Desk for advice. Depending on your requirements, a short-term loan laptop (without encryption or encryption hardware) may be available. In conjunction with Information Assurance Services, we will offer advice on recommended working practices which allow you to use this device as safely as possible while abroad.

Import licence required

Some countries require you to obtain an import licence if you are taking encryption hardware with you or using encrypted devices. In cases where encryption hardware is controlled, the licence will be required regardless of whether encryption is actually in use.

You will normally need to apply in advance for an import licence, generally at the same time as obtaining a visa. Some countries have individual exemptions for encryption hardware or software, be careful as these may be for private, non-business related purposes. If you are relying on an exemption you must be sure it will apply to you.
The process of obtaining an import licence for encryption may take longer than obtaining a visa for travel. By applying for an import licence, you may be advertising that you are carrying (potentially) sensitive information with you on your device and in some countries this may increase the risks that your device may be tampered with.

**Information Disclosure**

Even in countries where encryption is permitted (for example, the United States) you may find that you are required to allow local authorities access to your laptop or other storage devices and, if encrypted, that you disclose the encryption keys needed to access information on them.

You should plan ahead when travelling abroad and taking information with you on your laptop. You should not take any information with you where its disclosure to authorities would constitute a breach of [data protection legislation](https://www.gov.uk/government/guidance/data-protection-act-2018); a breach of confidence; or would otherwise be damaging to the interests of the University. As far as possible, any information you take with you should be limited to that which is necessary for your work while abroad.

**Tampering**

There are some countries where there are additional threats posed by the possibility of tampering. In these countries your laptop may be at risk of being compromised if it is handed to the authorities or is not kept with you at all times.

You are vulnerable even if the laptop is encrypted. It is possible for hardware key loggers to be installed so that your activities and communications (including your PIN and your username and password) can be recorded.
**Countries with known controls or issues**

This list was accurate at the time of publishing this page (January 2014) but the legal situation in other countries can change and you must not rely on it alone to take decisions.

As a general rule if you are travelling outside of the European Union you should check with the embassy of the country you are travelling to in advance. If you need a visa to travel, you should enquire when applying for your visa. If you do not need a visa to travel, you should check as far in advance of travelling as possible.

You can also email the Foreign & Commonwealth Office for advice at TravelAdvicePublicEnquiries@fco.gov.uk.

These countries require an import licence, ban encryption entirely or are countries where you may be at higher risk of your laptop being tampered with.

---

**Important:** We do not recommend travelling to countries where there is a high risk of tampering with an IT Services managed laptop or any other laptop you routinely use. If you are travelling into one of these countries and it is absolutely critical that you take a laptop with you, then you should contact the IT Service Desk for advice.

<table>
<thead>
<tr>
<th>Country</th>
<th>Licence required</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>Yes</td>
<td>High risk of tampering</td>
</tr>
<tr>
<td>Russia</td>
<td>Yes</td>
<td>High risk of tampering</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>Encryption may be banned</td>
<td>High risk of tampering</td>
</tr>
<tr>
<td>Belarus</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Burma (Myanmar)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Hungary</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Iran</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Israel</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Moldova</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Morocco</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Tunisia</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Ukraine</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Further advice

IT Services and Information Assurance Services are able to offer guidance on your options if you are travelling into a country with restrictions or controls. Contact the IT Service Desk in the first instance.

However, this is a complex area with different regulations across many different legal jurisdictions and we do not have legal specialists who can give definitive and safe travel advice. We are not a substitute for checking with either the Embassy of the country in question or the Foreign & Commonwealth Office in advance of your travel.