**St George’s, University of London**

**Travelling Abroad with your University Laptop Procedure**

**Purpose**

This document outlines the procedure for when a university encrypted laptop is used abroad. As well as protecting your information and yourself, this also ensures that you are complying with the University’s Information Security Policy and Remote Access Policy.

**Background**

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 a university laptop (or equivalent) with you, in others you should not take your laptop with you at all.

What you need to consider:

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

Legality: It may be illegal to use encryption or take encryption hardware into a country.

Import license: You may need an import license to use encryption or take encryption hardware into a country.

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.

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.

**TRAVELLING ABROAD**

**Countries where it is illegal to use encryption or take encryption hardware into it.**

As all University laptops are encrypted then where it is illegal to use encryption or take encryption hardware into a country then no University encrypted laptops or devices must be taken to these countries.

**Countries which you can freely enter with an encrypted laptop**

There are some countries which allow individuals to enter with encrypted laptops without the need to seek any license or permission (“Permitted Countries”). Permitted Countries grant individuals a “personal use exemption” to freely enter with encrypted laptops on the understanding that the individual does not create, enhance, share, sell or otherwise distribute the encryption software during his/her stay in the relevant Permitted Country.

Remember that even though you may not need a license to take an encrypted laptop into the Permitted Countries, upon entry you may still be asked to divulge the contents of your laptop by un-encrypting the laptop. See the “Practical Tips” section below for further advice in this regard.

**Countries for which you need permission to enter with an encrypted laptop**

If a country is not included in the list of Permitted Countries it is likely that an individual will need permission for their encrypted laptop; usually an import license will be required to enter the country with the laptop. Such import licenses are obtained by applying to the government of the country in question. Even with a license be conscious that your laptop may still be searched and you may be asked to un-encrypt. (see the “Practical Tips” section below).

Taking an encrypted laptop to certain countries without possession of the appropriate licenses could violate both UK export controls and/or the import regulations of the country being travelled to. This could result in the confiscation of the laptop, fines and/or other penalties.

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 laptops.

**Permitted Countries**

To check on a country’s permitted status with regards the import of an encrypted laptop you should check with either the embassy of the country you are going to visit or the Foreign, Commonwealth and Development Office in advance of your visit. The following link can be used as guidance only as it may not be current – [world map of encryption.](https://www.gp-digital.org/world-map-of-encryption/)

**Practical Tips**

Depending upon the country you are visiting and the security arrangement at its borders, you may be asked to reveal the contents of your laptop, storage device or papers. For this reason, you should never take any sensitive data where its disclosure to authorities would constitute a breach of data protection legislation; a breach of confidence; or would otherwise be damaging to the interests of the university.

* If it is an absolute necessity to take sensitive data overseas you must seek permission from your director and also from the Data Protection Officer if personal identifiable data is involved.
* back up any electronically stored data prior to your departure
* keep such data to the minimum necessary for the duration of the visit
* encrypt the storage device.
* keep the storage device secure

You must assume that any overseas government has the right to access your data and you should therefore be prepared to show it to them if necessary. If possible SGUL’s 'mydesktop’ should be used. You should also assume that all network traffic can be intercepted.

A university letter stating that the laptop/data is encrypted using commercial encryption software and that the information is normal business information in relation to the individual’s role at the university, may be helpful in the event of questioning at border controls. See Appendix 1.

**Responsibilities:**

The staff member taking the University laptop abroad:

* Is fully responsible for the security of the laptop
* Must have checked and noted the status of the country or countries to be entered with regards to restrictions on the import of encrypted laptops.
* Must seek approval from their line manager and notified them of any restrictions on taking the laptop into the country or countries to be visited.
* Confirm with IT services that only corporate software is installed on the laptop and that there are no licensing issues with the software being used abroad.
* Have in the 6 months prior to visiting the country or countries have taken and passed the university’s mandatory IG Training.

**Appendix 1.**

**TO BE PRINTED ON UNIVERSITY LETTER HEADED PAPER:**

**T**o whom it may concern

I, (Name and Position) St George’s, University of London (University) confirm that the bearer of this letter, (Name), (Position), is travelling with an encrypted laptop; the laptop has been encrypted (with standard, freely available encryption software) by the University as it contains sensitive commercial information relating to the University.

Yours Faithfully

(Name), (Position)

St George’s, University of London