UNIVERSITY OF SUSSEX

Travelling Abroad with University Information

Contents

Document Information

Document Title	**Travelling Abroad with University Information**
Release Date	04 Aug 2017
Version Number	0.3
Document Owner	Head of Technical Operations
Author	Peter Collier
Document Approval	IT Management Team
Approval Date	tbc
Review Plan	To be reviewed annually

1. Introduction

When travelling abroad and taking University information with you, you should plan ahead to ensure you and the information remain safe. As far as possible, any information you take with you should be limited to that which is necessary for your work while abroad.

You should not take any information with you 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.

Before travelling, you should also check what the import and custom requirements are of the destination country – some countries restrict the import of electronic devices or encrypted devices, while some reserve the right to require you to give them full access to electronic data you are carrying.

2. Purpose of this Document

This document provides help and guidance to any University staff, students or researchers who are planning to travel outside of the UK with electronic information - consideration should also be given to any paper material being carried that could be confiscated or lost in transit.

3. Guidance

What should I take with me?

The University recommends that you take the minimum equipment and information with you.

- Remove data from your device if it's not required
- Move information to the cloud any data that is not essential – the University provides you with access to cloud services such as Microsoft OneDrive and BOX.
- If you have concerns over Sussex email, you can remove the account from the device and use the webmail application https://webmail.sussex.ac.uk/.

Should I encrypt devices before I go?

It depends. Most countries allow individuals to enter with encrypted devices without the need to seek any licence or permission. However, even though you do not need a licence to take an encrypted device into these countries, you may still be asked to divulge the contents of the device, by unencrypting it at the point of entry.

For those countries where you need permission to enter with an encrypted device you will need some sort of import licence to bring it into the country. Such import licences are usually obtained by applying to the embassy of the country in question.

Be aware, though, that even with a licence, your device may still be searched and you may be asked to unencrypt it.

Note that taking an encrypted device to certain countries without possession of the appropriate licences could violate the import regulations of that country. 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 - before travelling internationally, it is important to ensure that you have the most up-to-date information about travelling with encrypted devices. You can obtain this from the embassy of the country.

Surely my smartphone will be safe?

In most countries, yes, but there are some countries where phone tapping and interference with devices in hotel rooms is a real possibility, including putting monitoring software onto the smartphone or tablet to obtain data remotely. In some cases it may be better to take a plain old phone-only handset that can't hold much information and cannot easily be breached.

It is also worth making sure you have backed up anything that is personally important to you – family photos for example – before you travel in case your phone becomes lost or stolen.

I haven't got time to strip all my data off my laptop – is there an alternative?

Yes – come and talk to IT Services who should be able to lend you a blank device for travelling with. The device will then be wiped on its return.

I need to take sensitive research or personal data with me, is that ok?

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 avoid taking any personal data relating to staff, students or research participants, and any confidential data that is subject to contractual constraints.

It is critical that you are aware of your obligations under Data Protection law – University guidance can be found at http://www.sussex.ac.uk/ogs/policies/information/dpa.

If it is necessary to take person identifying data overseas, you must:

- consult the Records Management Office in advance of your planned departure
- 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 or file(s)
- keep the storage device or papers 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. Otherwise you should avoid taking it and should discuss alternative arrangements with IT Services such as remote access and / or a temporary loan laptop and phone.

If you are researcher you should also be aware of the terms of any funding or data sharing agreements that you have in place which may contain restrictions.

How can I find out more about the country I'm going to?

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 or look at the website https://www.gov.uk/foreign-travel-advice for more country-specific information.

4. Revision history

Name	Date	Vers.	Change
Matthew Trump	27/06/2017	0.1	First draft version.
Matthew Trump	24/07/2017	0.2	Revised, shortened version with less emphasis on encryption.
Pete Collier	04/08/2017	0.3	Updated format and some revisions.