OCAD UNIVERSITY

# Security Considerations for International Travel with Mobile Devices

## Introduction

OCAD University employees should understand that special considerations may apply when encrypted devices are taken outside of Canada. Staff and faculty must be aware of restrictions to avoid the confiscation of their device, or other penalties. The following information is for reference only. All faculty and staff should contact the countries that they are planning to visit to determine what the requirements are in those jurisdictions.

Computers and laptops managed by OCAD U IT Services have encryption enabled on them. We recommend employees set up encryption on personally-owned devices if they are using them for OCAD U related work.

## How to Avoid Problems

Travelling to some countries with encrypted devices may not be advisable. You may want to contact IT Services well in advance (two to three weeks) of your travel if you wish to remove encryption or borrow a laptop (if available) that is not encrypted.

You can access most content in the cloud and would therefore not need to store it locally. However, you would need to remove the OCAD U OneDrive folders (or any cloud file storage service you use) mapped to your computer, as well as the Outlook Email Client (if installed), in order to not have any confidential or personal data stored locally on a laptop you use regularly. This can be resolved if you borrow a laptop, as nothing would be mapped or stored locally on that computer.

If you take your own laptop or other device, you should consider:

- Removing all confidential data on your laptop, tablet and phones including email, documents, photos and remove the configuration settings for these services from your device
- Disabling encryption software from the device
- Clearing your browser histories and caches
- Removing social media apps and configurations
- Considering whether it is necessary to take your mobile phone or other personal devices with you
- Not disabling geolocation software like Find My Mac or software that allows you to lock or disable your device remotely

## Providing Passwords to Law Enforcement Officials

In many countries, customs or other law enforcement officials are authorized to require travellers to unlock a device (including mobile phones) or produce a password. Refusal to comply may result in denial of entry, arrest, or confiscation of the device.

If asked by an official to unlock a device or provide a password, OCAD U employees should advise the official that the device contains confidential university information. If the official persists, the employee may comply with the demand. In such cases, the employee should make reasonable efforts to keep the device in sight at all times, and should change passwords and report such access to their OCAD U supervisor and IT Services, as soon as possible.

## OCAD U Assistance

Please contact the IT Help Desk at ithelp@ocadu.ca or ext. 277 for assistance when planning your travels.

## Additional resources:

### Encryption:

http://www.ocadu.ca/services/it/it-security/it-security-tips.htm

https://support-its.ocadu.ca/index.php?/Knowledgebase/Article/View/361/139/security-how-to-secure-your-computer-with-encryption

### Information & data classification policy:

http://www.ocadu.ca/Assets/content/it/OCAD+U+Information+and+Data+Classification+Policy.pdf

### Other resources related to international travel and digital devices:

https://www.eff.org/wp/digital-privacy-us-border-2017

https://cio.ubc.ca/sites/cio.ubc.ca/files/documents/resources/Sec%20Considerations%20for%20Intl%20Travel%20with%20Mobile%20Devices%20Guideline.pdf