UNIVERSITY
OF WOLLONGONG
AUSTRALIA

TRAVELLING OVERSEAS WITH DEVICES PROCEDURE

Date first approved: 19 August 2020	**Date of effect:** **19 August 2020**	**Date last amended:** (refer to Version Control Table)	**Date of Next Review:** 19 August 2023
First Approved by:			
Custodian title & e-mail address:	Senior Manager Client Services, Information Management & Technology Services Imts-admin@uow.edu.au		
Author:	Cyber Security Manager, Information Management & Technology Services Imts-admin@uow.edu.au		
Responsible Division & Unit:	Information Management & Technology Services		
Supporting documents, procedures & forms:	Cyber Security Policy IT Acceptable Use Policy IT User Account Management Procedures Privacy Policy Research Data Management Policy Student Conduct Rules Telephone and Mobile Use Policy University Privacy Statement & Policy		
Relevant Legislation & **External Documents:**	Crimes Act 1914 (Commonwealth)		
Audience:	Internal		

Submit your feedback on this policy document using the Policy Feedback Facility.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Contents

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

1 Purpose

1. This document sets out University procedures on travelling overseas with University Devices.
2. The targeting of Users using Devices whilst overseas is a real and ongoing threat. All Devices have the potential to be targeted.
3. The compromise of Devices could impact the ongoing operation and security of the University's business.
4. Generally, the risks associated with Device usage during overseas travel are:
    a. The compromise of Devices could give unwanted access to personal or University data. This could immediately impact the integrity, confidentiality or operational security of the University's business activities;
    b. The compromise of Devices could allow external access into any connected networks putting additional University data at risk; and
    c. The compromise of Devices could result in immediate or ongoing operational security or safety concerns for targeted Users.
5. The University of Wollongong is committed to the appropriate use of Information Technology and Services to support its learning, teaching, research, administrative, and service functions. The IT Acceptable Use policy defines acceptable behaviour expected of Users of University IT Facilities and Services. The University requires Users to comply with the IT policies and associated requirements governing the Use of IT Facilities and Services as a condition of their use. These are accessible on the University Policy Directory.

2 Definitions

Word/Term	Definition (with examples if required)
Clean Travel Device	A Device that has been wiped of any stored data.
Device	Any device that is provided to University staff and paid for by the University for the purposes of fulfilling individual work requirements.
Other Device	Any device, including personal devices, or any device that is provided to you for use by organisations or institutions other than UOW.
IMTS	Information Management & Technology Services at the University of Wollongong.
IT Facilities & Services	Information Technology facilities operated by or on behalf of the University. This includes services and systems and associated computing hardware and software used for the communication, processing and storage of information.
University	University of Wollongong and controlled entities.
User	A person assigned a User Account by the University or a person who is otherwise authorised to use University IT Facilities and Services.

3 Requirements

Prior to travel

1. Users are required to contact the IMTS Service Desk a minimum of ten (10) business days in advance of scheduled overseas travel, advising:
    a. Travel dates;
    b. Countries being visited;
    c. Whether any University data will be taken during the overseas travel (must only be stored on IMTS managed devices); and
    d. Whether there will be any need to access any University data (including email) remotely.
2. Users must ensure any personal Electronic Devices are up to date in terms of Operating System updates and patches are protected via a PIN, pattern or biometric factor such as a fingerprint.
3. Based on the information provided in 3.1, IMTS may need to issue the User with a Clean Travel Device for travel.

During Travel

4. Users must report any loss, suspected compromised or unusual behaviour (including the type, date and time) on Devices to IMTS as soon as possible.
5. Users must assume any Devices that have been taken out of sight for inspection by foreign government officials, or have been lost or stolen and later found or returned, to be potentially compromised.
6. Users must never lend Devices to untrusted people, even if only briefly. (An example would be if an untrusted person asked to check the weather on your device).
7. Users must never allow untrusted people to charge Other Devices using your Devices (An example would be if an untrusted person asked to charge their phone using your laptop).
8. Users must never use chargers supplied by third parties or charge Devices at designated charging stations or USB charging outlets. Users are required to only use genuine chargers supplied with Devices.
9. Users must never place Devices, including multi-factor authentication tokens, in check-in luggage. Users must never leave Devices, including multi-factor authentication tokens, or luggage containing such items, unattended, even in hotel safes.
10. Users are required to avoid connecting Devices to any open or public Wi-Fi networks, and must always use the UOW VPN to ensure all of your internet traffic is encrypted.
11. Users must disable any communication capability for Devices when not in use. This includes cellular data, Wi-Fi, Bluetooth and Near Field Communication (NFC).
12. In locations where sensitive conversations take place, Users must power-down Devices and remove them from close proximity to the sensitive conversations.
13. Users must avoid re-using removable media after connecting it to other organisation's Electronic Devices, as they may not provide the same level of security as UOW, or their Electronic Devices could be compromised.

14. Users must ensure that they run a manual antivirus scan on any removable media before opening any files on it.
15. When travelling overseas or when returning to Australia users must never use any Other Devices that have been gifted or loaned to them, especially removable media. If required, Users must purchase Other Devices from established and reputable local businesses.

Returning From Travel

16. Users must return Clean Travel Devices to IMTS, to be wiped and returned to factory default.
17. At no time may Users connect Clean Travel Devices to the UOW network upon return from travel.
18. If required, the transfer of any data obtained by the User on a Clean Travel Device whilst travelling, will be completed by IMTS.

4 Roles & Responsibilities

IMTS

1. IMTS will ensure laptops are patched and running all appropriate Antivirus and protection software and running hard disk encryption.
2. IMTS will ensure that a Company phone is password/fingerprint protected.
3. If University data needs to be stored/taken a Clean Travel Device that contains no identifying marks/stickers, should be provided by IMTS instead of the User's day-to-day Device being used.

All Users

1. Users must ensure all appropriate steps within this document are being followed.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

5 Version Control and Change History

Version Control	Date Effective	Approved By	Amendment
1	19 August 2020	Chief Operating Officer	First version