Acceptable Use

1 POLICY STATEMENT AND PURPOSE

The purpose of this policy and guidelines is to outline appropriate acceptable use parameters for use of ICHM IT Resources, to ensure the continued effective and secure operation of those IT Resources. This includes protecting ICHM from issues related to security, error, fraud, defamation, copyright, discrimination, bullying, illegal activity, privacy, and service interruptions.

The use of ICHM IT Resources is integral to the provision of a successful learning environment underpinned by technology enhanced learning at ICHM. All students are responsible for ensuring that our supportive teaching and learning environment is enhanced by the proper and considerate use of information technology and associated resources.

2 SCOPE

This policy applies to all ICHM students.

3 DEFINITIONS

Technology Enhanced Learning (TEL) - TEL is any learning that occurs through the application of electronic communications and computer-based educational technology, combined with pedagogical principles and practices that are applicable to and tailored for this purpose

ICHM IT Resources – includes, but is not limited to, all systems and IT equipment (servers, Software, Cloud Services, collaboration platforms, mobile devices etc.), used to store, manage, or transmit ICHM information.

BYOD (Bring Your Own Device) – a Mobile Device owned by the Student User to access ICHM IT Resources.

Cloud Services – includes, but is not limited to, software or services that are leased on a subscription basis.

Mobile Device – a device which may be able to communicate over the mobile data network or Wi-Fi networks (for example, mobile phones, iPads, Android tablets, mobile data cards) and provides communication and access to IT Resources. These may be ICHM owned or personally owned by the Student User (BYOD).

User Devices – includes any device accessing ICHM IT Resources (for example tablets, computers, Mobile Devices etc.).

Security Controls – safeguards or countermeasures to detect, counteract, or minimise security risks and ensure legal compliance to ICHM IT Resources. Includes, but is not limited to, technical controls such as passwords and administrative controls such as policies.

4 POLICY DETAILS

Access to IT Resources

All enrolled ICHM students are supplied with a network login for access to email and the Internet, for educational or Work Integrated Learning Placement related purposes only.

By accepting a login to the ICHM IT Resources, ICHM students accept the responsibility to use those resources according to this Acceptable Use Policy

a) Access to ICHM IT Resources is controlled using User IDs, passwords and two factor authentication. All User IDs and passwords are uniquely assigned to named individual students and consequently, students are accountable for all actions associated with their IDs.

b) Password Complexity:

- Passwords must be at least 10 characters in length;
- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters; and
- Cannot be the same as previous passwords
- Must contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)

c) c) Individuals must not:

- Allow anyone else to use their user ID/token and password;
- Leave their user accounts logged in at an unattended and unlocked computer;
- Use someone else's user ID and password to access ICHM IT Resources;
- Leave their password unprotected (for example writing it down);
- Perform any unauthorised changes to ICHM IT systems or information;
- Attempt to access data that they are not authorised to use or access;
- Store ICHM data on any unauthorised equipment; or
- Give or transfer ICHM data or software to any person or organisation outside ICHM.

Use of ICHM IT Resources

Individuals must not:

- Use ICHM IT Resources to create, store, access, or copy information for the purposes of harassment or abuse;
- Use profanity, obscenities, or derogatory remarks in communications;
- Access, download, send or receive any data (including images), which ICHM considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material;
- Place any information on the Internet that relates to ICHM or alter any information about it, unless they are specifically authorised to do this;
- Download copyrighted material or breach licensing agreements; or
- Download any software onto ICHM IT Resources from the internet.

Personal Computers supplied by ICHM Pty Ltd to students

Students can request to be provided with an ICHM computer, for a limited period, by a written request to the Program Director Academic. Where approved, the computer will be provided for study purposes only and must be used in accordance with the requirements of this Acceptable Use Policy.

Inappropriate use of an ICHM computer, the ICHM network and/or the internet may result in the imposition of restrictions or termination of access.

All ICHM supplied equipment is provided for the purposes of your study and you are responsible for this device while it is in your possession. You must keep it secure, and any loss or damage should be reported immediately to the Program Director Academic. You must not leave devices unattended in public places or visible in parked cars.

Email and Personal File Storage

Students are provided with an ICHM email address, webmail account and a generous personal file storage facility (OneDrive) through Microsoft Exchange. Access to email and personal folders is available from anywhere in the world 24 hours a day

Students are expected to read their student emails/messages daily, or more often, during the semester and examination period. Official emails/messages are understood to have been received and read.

Those on Work Integrated Learning (WIL) placement are encouraged to check their webmail daily but must do so at a minimum, every 5 days.

Official email communications from ICHM administration or lecturing staff are sent via Microsoft

Students are discouraged from redirecting their ICHM email to other personal email accounts but may do so if they wish. ICHM accepts no responsibility for messages not forwarded to personal accounts because of systems failure or omission.

Monitoring and Filtering

a) IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy.

b) ICHM has the right to monitor activity on its systems, including internet and email use, to ensure systems security and effective operation, and to protect against misuse.

c) ICHM is not responsible for any loss you suffer if any of your personal files or personal email is lost from ICHM IT Resources.

Antivirus

a) Some material delivered by email may be deemed unsuitable or present a risk to the business. This can be due to attachments that contain trojans, worms, viruses, or other malware, or due to emails containing spam or originating from known spam sites.

b) A system generated email will notify you of the barred message and the reason. If you require access to any emails barred by the email filtering software, then please contact the IT Helpdesk.

IT Support

Student access IT support by logging IT requests with the Helpdesk via https://support.up.education/ or via email on helpdesk@up.education, or call the 0800 463 448 (urgent problems or escalations) number from NZ or +64 9 558 4692 from Australia to talk to the on-call support staff. You will need to provide the Helpdesk ticket number to the on-call staff so that they can assist you efficiently.

5 SUPPORTING DOCUMENTATION

Not applicable.

6 RESPONSIBILITIES AND AUTHORITIES

The UP Shared Services IT Team is the policy owner and the CEO is responsible for approving this policy.

7 REVIEW

The UP Shared Services IT Team is responsible for the review of this policy on a 3 yearly basis, as per the Policy Register.

8 ACKNOWLEDGEMENT (if applicable)

TEQSA – Guidance Note: Technology Enhanced Learning

UP Education Group Policy Acceptable Use

9 APPROVAL

COMPUTERS AND INTERNET	
Policy Owner	UP Shared Service IT Team
Version Number	6.0
Approval Authority	Chief Executive Officer
Approval Date	21 February 2022
Next Review Date	February 2025
Superseded Document	Computers and Internet Policy

Version Control and Modification History Table				
Date	**Version**	**Modification**	**Approval Authority**	**Approved & Published Date**
18/01/2012	1.0	Modification of existing policy	Roger Stevens and Dr Ian Whyte	18/01/2012
06/11/2012	2.0	Addition of changes to the policy section	Dr Ian Whyte and Gerald Lipman	06/11/2012
07/01/2014	3.0	Change reference to degree to include all courses-recommended by TEQSA in letter 19/12/2013	Dr Ian Whyte and Gerald Lipman	07/01/2014
08/02/2016	4.0	Revised to reflect agreement now with ICHM	Dr George Brown	08/02/2016
21/01/2020	5.0	Increased internet quota and removed Desktop PC and PC specifications	Dr George Brown and Natalie Simmons	10/03/2020
Feb 2020	5.1	Change to position titles	CEO and Principal	May 2020
20220221	6.0	Major amendment Edits for amended reference to ICHM, position titles, applicability to all students regardless of study mode, course, clarity, order and consistency. Major update to sector language and alignment with UP Group IT support and Acceptable Use Policy.	CEO	21/2/2022