Academic

Computers and Internet Policy and Procedure

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 programs-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

1 POLICY STATEMENT AND PURPOSE

The use of computers and the internet is integral to the establishment and continuous development of a successful teaching and learning environment in the ICHM programs. Individuals are responsible to ensure that this successful teaching and learning environment is enhanced by the proper and considerate use of computing and internet resources.

2 SCOPE

This policy applies to all ICHM students.

3 DEFINITIONS

Not applicable.

4 POLICY DETAILS

Computer Use

All enrolled ICHM students will be supplied with a network login for access to email and the Internet, for educational or work related purposes only.

By accepting a login to the ICHM computing facilities, ICHM students accept the responsibility to use those facilities according to specific institute policies established for computer operations on and off campus. ICHM students will be required to read and acknowledge the *User Agreement* when logging on to the ICHM network for the first time each semester.

A copy of the *ICHM User Agreement* is found at *Appendix A.*

Personal Computers supplied by ICHM Pty Ltd to students resident in Regency International House (RIH)

Students of ICHM residing in RIH will be provided with **limited access** (20GB per month, not cumulative) to the internet through a private network from their bedrooms and may request to be provided with the use of a personal desktop computer. Primarily provided for study purposes, students may use the network for a wide range reasons, including for personal use, social networking and entertainment. Additional access to the internet may be purchased from RIH Reception.

Inappropriate use of the ICHM network and/or the internet may result in the imposition of restrictions or termination of access. Users will be issued a unique user name and password for the computer and for access to the internet which may not be shared with others.

Email and Personal File Storage

Students will be provided with a College 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.

Microsoft Outlook is the primary communication vehicle between administration and lecturing staff and students, whether on or off campus. Students of ICHM, therefore, are required to read their incoming messages daily, or more often, during the semester and examination period. Official messages sent to students' College email will be deemed to have been received and read within 24 hours of their having been sent.

Those on WIL are encouraged to check their webmail daily but must do so at a minimum, every 5 days.

Official communications from ICHM administration or lecturing staff will only be via Microsoft Outlook. Students are discouraged from redirecting their email to other personal email accounts but may do so if they wish. ICHM will take no responsibility for messages not forwarded to personal accounts as a result of technological failure or omission.

Support

Problems with hardware (the computer, display or peripherals) or the software (programs or settings) should be reported to RIH Reception where a Maintenance Request Form should be completed. Please be specific and provide as much information as possible. A service technician will be available weekly to attend to these reports.

While every effort will be made to ensure a stable network, it is your responsibility to take proper precautions to protect your personal files by backing up regularly in your OneDrive folder.

Privacy

You should be aware that the following data is recorded:

- Date and time of log-in
- One or both signed User Agreements
- The computer name and number
- Your unique identification number

Appendix A

USER AGREEMENT

I undertake to ensure that my PASSWORD is kept confidential**,** and acknowledge that unauthorised use of my personal USER - ID may result in the integrity of the system being compromised. I further accept that I am responsible for ensuring my personal USER - ID is not shared and is only used for proper and authorised activities.

I have read and understand the Policies for use of computing facilities and I will observe and be bound by the conditions of the policy at all times. I undertake that if there is access to any services associated with my account for which charges are payable in addition to the basic Internet access charge, I will pay ICHM all such charges, unless specifically authorised to incur this cost.

1. Access is for official or designated duties and not for private, business or political purposes.

2. All data stored on any machine or network remains the property of ICHM and can be accessed, and / or removed at any time.

3. Not intentionally or by negligence, must you divulge to any person the password(s) associated with your login, or allow others to use that login.

4. Always logout of the system when leaving a workstation. You are liable for the use of the computing facilities at all times when you are logged in.

5. No software or applications are to be loaded/downloaded, used or stored on the computers unless licensed to ICHM, and then only following agreement from the IT Officer.

6. Unless specifically authorised, do not intercept, download or attempt to electronically read another user's files, transmissions or electronic mail.

7. The principles of conduct apply to all employees when using e-mail, the Internet or engaging in any other related activity.

8. Specifically, the access, transmission, retrieval, storage or display of:
    - sexually explicit material
    - hate speech or offensive material
    - material regarding illicit drugs or violence
    - material regarding criminal skills and/or illegal activities
    - material of a defamatory, discriminatory or harassing nature

    is strictly forbidden if that material does not form part of a legitimate educational inquiry.

    This includes accessing any sites or forums that deal with these materials. Any such material stored on network file servers or on departmental computers will be removed. Non-compliance with these directives may give rise to a charge of improper conduct and any such material may be used as evidence in misconduct/disciplinary proceedings against an employee or student. Furthermore, any material found that may be related to child pornography or paedophilia will be referred to the SA Police and may lead to a criminal charge.

9. ICHM reserves the right to monitor e-mail and Internet activity undertaken, using resources provided by ICHM. This will also apply to situations where access to the Internet or e-mail at home or elsewhere using ICHM equipment and/or Internet service. Systematic audits of Internet and e-mail usage will be conducted.

10. Do not breach State and Commonwealth laws or regulations on Equal Opportunity, Sexual Harassment, Copyright, Electronic Access or Privacy in your use of ICHM computer systems.

11. Software and/or applications in operation are licensed only for ICHM use. They may not be copied for further distribution.

12. Users are not to use software or applications that are not part of those specified for their respective enrolment group. This includes network commands.

13. Users must not attempt to rectify equipment or network errors by connecting or disconnecting cables or changing configuration files.

14. Users of the computing facilities must not in any way, attempt to modify any software or hardware settings that may alter the integrity of the computer. Attempting to set illegal passwords on files, BIOS set-up or any other configuration will result in instant revoking of your network login.

Please Note:

Users are advised not to store any data on the Hard Disk drive of the computer in use as this data is not backed up and cannot generally be retrieved if the hard drive fails. Users that do store data on the computer / laptop hard drive must store a copy on OneDrive in the cloud so it can be backed up and restored following a disaster such as a hard drive failure.

The consequences of not following the Policies regarding the use of ICHM computing facilities could result in down time of the system - at a great cost of time and money to ICHM and other users.

User behaviour and practices are constantly monitored by the system and by the staff of ICHM.

Disciplinary action will be taken against any user found to be in breach of this policy for use of the computing facilities.

A breach of policy may require staff or students to meet with the Principal and/ or Chief Executive Officer, to discuss the details of the breach. Ignorance of the policies will not be accepted as an excuse for violation of the agreement.

5 SUPPORTING DOCUMENTATION

Not applicable.

6 RESPONSIBILITIES AND AUTHORITIES

The Principal is the policy owner and the Chief Executive Officer is responsible for approving this policy.

7 REVIEW

The Principal is responsible for the review of this policy on a 3 yearly basis, as per the Policy Register.

8 ACKNOWLEDGEMENT (if applicable)

Not applicable.

9 APPROVAL

COMPUTERS AND INTERNET	
Policy Owner	Principal
Version Number	5.1
Approval Authority	Chief Executive Officer
Approval Date	May 2020
Next Review Date	May 2023