ICT POLICY

Approving Authority	Council	**Approval Date of Last Revision**	6 May 2019
Approval Date	15 Dec 2017	**Effective Date of Last Revision**	6 May 2019
Effective Date	15 Dec 2017	**Review Date***	15 Dec 2020
Document No	PLO5	**Version**	1.0a
Policy Category	Operational		
Governing Authority			
Responsible Officer	General Manager		
Related Documents	ICT Procedure Staff Code of Conduct Student Code of Conduct Records Management Policy Privacy Policy Criminal Code Act 1995 (Cth) Spam Act 2003 (Cth) Copyright Act 1968 (Cth) Telecommunications (Interception and Access) Act 1979 (Cth)		

** Unless otherwise indicated, this Policy will still apply beyond the review date.*

Contents

Document Control

Version #	Date	Key changes
1.0	15/12/2017	Approved by Council
1.0a	6/05/2019	Format updated

1. PURPOSE

1.1 The Information and Communication Technology (ICT) Policy sets out the rules applicable to the use of information and communication technology resources at Adelaide Institute of Higher Education (AIHE).

1.2 The Policy expresses the commitment of AIHE to providing and maintaining secure, effective and reliable ICT facilities, services and infrastructure to support the daily operations, learning and teaching at AIHE.

2. SCOPE

2.1 This Policy applies to all staff and students of AIHE. It applies to users of AIHE equipment and to users connecting personally owned devices, such as laptop computers, smartphones and tablets, to the AIHE network and/or storing any AIHE data on such devices.

3. POLICY STATEMENT

3.1 ICT facilities, services and infrastructure are provided in support of AIHE business including teaching and learning, and operational activities.

3.2 AIHE ICT resources will support learning activities and provide students with opportunities for academic interactions outside of formal teaching.

4. PRINCIPLES

4.1 Provision of ICT Facilities, Services and Training

4.1.1 AIHE seeks to provide its staff and students with secure and timely access to ICT equipment and the online services and resources necessary for undertaking their work and study.

4.1.2 Students are required to supply and bring their own device for their study at AIHE. Details of device requirements and specifications will be provided in the student's Letter of Offer.

4.1.3 AIHE will provide staff and students with timely access to the Learning Management System and make training available in the use of the system.

4.2 Acceptable and Unacceptable Use of ICT

4.2.1 AIHE facilities and services must be used in a lawful, ethical and responsible manner, and in accordance with the ICT Acceptable Use Schedule (see Schedule A), other applicable policies, and any additional terms of use that may apply to particular software or services.

4.2.2 AIHE ICT facilities and services are provided for use in the academic, administrative, commercial and community activities of AIHE. Some reasonable non-commercial personal use may be allowed; however, this is a privilege and not a right, and if that privilege is abused it will be treated as a breach of this Policy.

4.2.3 Account holders must take all reasonable steps to protect their account from unauthorised use.

4.2.4 Use of AIHE ICT facilities and services or bring your own devices (BYOD) must not jeopardise the fair, secure, and productive ICT environment of the AIHE community, nor AIHE's operations, assets, data integrity or reputation.

4.2.5ICT u sers must not install or use unlicensed or malicious software on AIHE ICT facilities and services or BYOD, nor circumvent AIHE's ICT security measures.

4.2.6ICT u sers are expected to report actual or suspected breaches of this Policy or other security incidents that may be a threat to the security of AIHE ICT facilities and services in a timely manner.

4.3 Administering AIHE ICT Facilities and Services

4.3.1 Provisioning and de-provisioning of AIHE User IDs and other access to AIHE ICT is governed by formal business rules administered by Technology Services, Human Resources and Student Services.

4.3.2 AIHE may impose volume quotas (e.g. printing, file storage, downloads) and security measures on the use of AIHE ICT facilities and services.

4.3.3 Normal operation and maintenance of AIHE ICT facilities and services includes logging of usage and activity on AIHE ICT facilities and services. AIHE may monitor and analyse such logs where it is reasonable for AIHE to do so, and to meet AIHE's legal obligations.

4.4 Security of AIHE ICT

4.4.1 AIHE will take all reasonable steps to protect the security of AIHE ICT facilities and services, including its confidentiality, integrity and availability.

4.4.2 AIHE will implement and operate an information security governance framework to effectively manage the security of AIHE ICT facilities and services.

4.4.3 The ICT Manager is ultimately responsible for the security of AIHE ICT. For AIHE ICT resources not managed by AIHE Technology Services unit, the respective ICT custodians are responsible for the implementation and management of this Policy and ICT Procedure in relation to AIHE ICT resources managed by their area.

4.4.4 Where there is a threat to AIHE ICT facilities and services or security, or if the use of AIHE ICT facilities and services presents a risk to AIHE, AIHE may take any necessary action to mitigate the risks, with or without prior notice.

4.4.5 Acquisitions of, and changes to, AIHE ICT facilities and services should not expose AIHE to unacceptable levels of information security risk.

4.4.6 The security of AIHE ICT facilities and services is maintained to protect AIHE's operations and information assets. ICT users should not use systems outside of AIHE ICT facilities and services to conduct AIHE business unless there is a genuine need to do so.

4.5 Breaches of the ICT Policy

4.5.1 Breaches of the ICT Policy may result in suspension of access to AIHE ICT facilities and services and/or;

- in the case of AIHE staff, may constitute misconduct, which will be addressed in accordance with AIHE's Enterprise Agreement or relevant AIHE disciplinary procedures;

- in the case of students, may constitute misconduct under the Student Code of Conduct.

4.5.2 Breaches of this Policy may also be reported to external parties as required under law.

5. ROLES AND RESPONSIBILITIES

5.1 All AIHE ICT users and account holders are responsible for protecting the security of AIHE ICT facilities and services by abiding by all relevant laws, AIHE policies and procedures and the ICT Acceptable Use Schedule (see Schedule A).

5.2 The ICT Manager is responsible for the of AIHE ICT facilities and services.

6. DELEGATIONS OF AUTHORITY

Authority	**Delegation Holder**
Authority to approve exceptions to this Policy	General Manager
Authority to grant visitor access to the AIHE ICT facilities and services	General Manager and Head of Business School
Authority to authorise the creation of generic, casual, and external visitor accounts	General Manager and Head of Business School
Authority to authorise a change to the level of access for staff, titleholder or visitor account	General Manager and Head of Business School
Authority to request examination of an account holder's use of ICT Facilities	General Manager and Head of Business School
Authority to approve Peer to Peer software for lawful purposes	General Manager, ICT Manager and Head of Business School
Authority to order the immediate suspension or termination of a staff, title-holder or visitor account	General Manager, ICT Manager and Head of Business School
Authority to order the immediate suspension or termination of a student account	General Manager, Student Support Officer, Lecturers, ICT Manager
Authority to immediately suspend or disconnect any account or ICT Facility based on an immediate threat to AIHE.	General Manager, Student Support Officer, ICT Manager, Lecturers
Authority to approve changes to the stand-alone procedures related to this Policy.	General Manager and Head of Business School

7. DEFINITIONS

7.1 See the AIHE Glossary of Terms for definitions.

SCHEDULE A – ACCEPTABLE USE OF AIHE ICT FACILITIES AND SERVICES

A person using AIHE ICT facilities and services is responsible for ensuring that they comply with the AIHE ICT Policy and related Procedure.

Appropriate use of AIHE ICT facilities and services includes but is not limited to:

(a) You shall use AIHE ICT facilities and services in a manner that is ethical, lawful and not to the detriment of others.

(b) You shall use only those AIHE ICT facilities and services you have been authorised to use.

(c) You shall only access ICT facilities and services on sites with AIHE's permission and in a manner consistent with the owner's conditions of use.

(d) You shall actively defend your access to AIHE's ICT facilities and services from unauthorised use by others, including complying with the Password Policy (by keeping your password secret).

(e) When using AIHE ICT facilities and services you shall produce your AIHE ID card if requested to do so by an authorised member of staff.

(f) You shall abide by instructions given by the ICT Manager or by their delegate. Such instructions may be issued by notice displayed near ICT facilities, by letter, by electronic communication, in person or otherwise.

(g) When you cease to be an enrolled student or an employee of AIHE, your access to AIHE ICT facilities and services will be terminated without notice. You are responsible for personal information you have stored on AIHE ICT facilities and services and must make arrangements for its retention and/or removal as appropriate prior to leaving AIHE. Note that AIHE records may only be disposed of in accordance with the Records Management Policy.

(h) You may use AIHE facilities and services for incidental personal use (e.g. occasional emails and web browsing during work breaks) provided that such use does not interfere with AIHE business operations, does not breach any Federal legislation, State legislation or AIHE policy or an ICT vendor's conditions of use or licence agreement. Some examples of interference with AIHE business operations include: disrupting ICT facilities or services; burdening AIHE with significant costs; or impeding one's work or other obligations to AIHE.

What not to do…

(i) You shall not obstruct others in their use of AIHE ICT facilities and services to achieve the functions and objectives of AIHE. Obstructing others includes the inappropriate use of ICT resources for activities such as, but not limited to:

- party-political activities;
- tying up computer resources for game playing;
- waging or betting or other trivial applications;
- sending harassing or frivolous messages, such as chain letters, junk mail and other types of broadcast material, either locally or over the Internet;
- knowingly accessing or sending sexually explicit, pornographic or otherwise offensive material; and
- using without thought, excessive amounts of storage.

(j) You shall not misuse the AIHE ICT facilities and services for harassment including but not limited to unlawful harassment such as sexual harassment. Further details of what constitutes harassment may be found in the AIHE Anti-harassment Policy.

(k) You shall not use any account that has been created for another ICT user without authorisation, nor shall you attempt to find out the password of another ICT user, access or alter information, services, usernames, or passwords without authorisation.

(l) You shall not attempt to subvert security measures in any way, nor use a false identity when using ICT facilities and services.

(m) Without the explicit authorisation of the ICT Manager, you shall not possess any tools nor undertake any activities on AIHE ICT facilities and services facilities or services that could result or assist in the violation of any AIHE policy, software licence or contract. Examples of these prohibited tools include viruses, Trojan horses, worms, password breakers, network packet observers or sniffers. Examples of prohibited activities include creating ping floods; spoofing packets; performing

denial-of-service attacks; forging routing information for malicious purposes; scanning for vulnerabilities; or other computer hacking techniques.

(n) You shall not attempt to adversely interfere with the operation of any of the AIHE's ICT facilities and services. For the purposes of this document, interfering includes wilful physical damage, wilful destruction of information, wilful interruption of normal operations, and accessing server areas without the permission of the ICT Manager.

(o) You shall not wilfully waste ICT resources. For example, wasting network bandwidth by downloading or sending large amounts of material that is neither work-related nor study-related.