ADELAIDE INSTITUTE of HIGHER EDUCATION

Policy PLO5

ICT POLICY

Approving Authority	Council	**Approval Date of Last Revision**	17 September 2026
Approval Date	15 Dec 2017	**Effective Date of Last Revision**	17 September 2026
Effective Date	15 Dec 2017	**Review Date***	17 September 2031
Document No	PLO5	**Version**	2.0a
Policy Category	Operational		
Governing Authority	Council		
Responsible Officer	Chief Executive Officer		

Contents

Purpose 1
Scope 1
Policy Principles 1
Roles and Responsibilities 2
Related Documents 3
Definitions 3

Purpose

1. This Policy establishes the principles governing the provision, use, security and management of information and communication technology (ICT) facilities and services at AIHE, to support teaching, learning and institutional operations.

Scope

2. The Policy applies to:
   - all staff, students and other authorised users of AIHE ICT facilities and services
   - all ICT facilities, services and systems provided, managed or authorised by AIHE, and
   - personally owned devices used to access AIHE ICT facilities and services or to access, store or process AIHE information.

Policy Principles

3. The following principles govern the provision, use, security and management of ICT facilities and services at AIHE:

   3.1 ICT facilities and services must support AIHE's teaching, learning and institutional operations and be appropriate, reliable and accessible for their intended purposes.

   3.2 AIHE will provide staff and students with appropriate access to ICT facilities, services and systems required for their work or study, together with appropriate information, support and training.

   3.3 ICT facilities and services must be used lawfully, ethically and responsibly, in accordance with this Policy and associated Procedure, other applicable AIHE policies and procedures, and relevant licence and service conditions.

3.4 ICT users must take reasonable steps to protect their accounts, access credentials, devices and information from unauthorised access or use, and must comply with ICT security requirements and controls established by AIHE.

3.5 AIHE information must be accessed, stored, processed, transmitted and disposed of in a manner that appropriately protects its confidentiality, integrity, availability and privacy.

3.6 Personally owned devices used to access AIHE ICT facilities and services, or AIHE information, must comply with applicable AIHE security requirements and must not compromise the security, integrity or operation of AIHE ICT facilities and services.

3.7 AIHE will implement appropriate technical and administrative controls to protect ICT facilities, services and information from unauthorised access, loss, misuse, interference, disruption and other security threats.

3.8 AIHE may log and monitor the use of its ICT facilities and services where this is lawful, reasonable and proportionate for purposes including maintaining security and system performance, investigating suspected misuse, meeting legal or regulatory obligations, and protecting AIHE information and assets.

3.9 Actual or suspected ICT or information security incidents, including loss or unauthorised access, use or disclosure of AIHE information, must be reported promptly and managed in accordance with the ICT Procedure and other applicable AIHE requirements.

3.10 ICT systems and services, including externally provided or cloud-based services, must be selected, implemented and managed with appropriate consideration of information security, privacy, continuity and institutional risk.

3.11 AIHE may take reasonable and necessary action, including restricting or suspending access to ICT facilities and services, where this is required to protect AIHE systems, information, users or operations from an actual or suspected threat.

3.12 Suspected breaches of ICT requirements will be assessed and managed in accordance with the ICT Procedure and, where applicable, relevant staff or student conduct processes. Matters may also be referred to external authorities where required by law.

4. The AIHE ICT Procedure gives effect to this Policy and sets out the operational requirements and processes for the use and management of ICT facilities and services. It covers user accounts and access security, personally owned devices, information and data security, monitoring and logging, ICT and information security incidents, breaches of ICT requirements, and backup, recovery and disposal.

Roles and Responsibilities

5. Council is responsible for oversight of significant ICT and information security risks as part of AIHE's institutional risk management arrangements.
6. The Chief Executive Officer is responsible for institutional oversight of ICT facilities and services and for ensuring that this Policy and associated Procedure are implemented appropriately.
7. The ICT Manager is responsible for the operational management and security of AIHE ICT facilities and services, including:
   - implementing and maintaining appropriate ICT and information security controls
   - managing user access and system security
   - monitoring ICT facilities and services and responding to ICT and information security incidents
   - supporting appropriate backup, recovery and continuity arrangements, and
   - providing advice and support on ICT and information security requirements.
8. The Head of School is responsible for ensuring that ICT used in teaching and learning is used appropriately and supports the effective delivery of courses and subjects.

9. Staff, students and other authorised ICT users are responsible for:
    - using AIHE ICT facilities and services lawfully, ethically and responsibly
    - taking reasonable steps to protect their accounts, access credentials, devices and AIHE information
    - accessing and using only ICT facilities, services and information for which they are authorised, and
    - promptly reporting actual or suspected ICT or information security incidents.

Related Documents

10. Related documents include:
    - AIHE ICT Procedure
    - AIHE Privacy Policy
    - AIHE Records Management Policy
    - AIHE Staff Code of Conduct
    - AIHE Student Code of Conduct
    - approved ICT standards, guidelines and related resources referred to in the AIHE ICT Procedure.

Definitions

11. Definitions for terms used in this Policy are contained in the AIHE Glossary of Terms.

Document Control		
Version #	**Date**	**Changes**
1.0	15/12/2017	Approved by Council
1.0a	6/05/2019	Format updated
1.0a	17/06/2021	Reviewed - no changes
2.0	17/09/2026	Significant reformatting and editing to focus on ICT principles and to better align policy and related procedure.
2.0a	17/09/2026	Approved by Council

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