ADELAIDE INSTITUTE of HIGHER EDUCATION

Procedure PRO5.1

ICT PROCEDURE

Approving Authority	CEO	**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 2029
Document No	PRO5.1	**Version**	2.0a
Policy Category	Operational		
Governing Authority	CEO		
Responsible Officer	ICT Manager		

Contents

Purpose 1
Scope 1
Access to and Use of ICT 1
User Accounts and Access Security 2
Personally Owned Devices 3
Information and Data Security 3
Software, Systems and External Services 3
Monitoring and Logging 4
Reporting ICT and Information Security Incidents 4
Responding to ICT and Information Security Incidents 5
Breaches of ICT Requirements 5
Backup, Recovery and Disposal 6
Related Documents 6
Definitions 6

Purpose

1. This Procedure gives effect to the AIHE ICT Policy and sets out the operational requirements for the use, security and management of AIHE ICT facilities and services and AIHE information.

Scope

2. The Procedure 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.

Access to and Use of ICT

3. AIHE ICT facilities and services are provided primarily for activities associated with AIHE's teaching, learning and institutional operations. Reasonable incidental personal use is permitted

provided that it does not interfere with AIHE activities, impose unreasonable costs or demands on ICT resources, or otherwise breach this Procedure.

4. ICT users must:
   - use ICT facilities and services lawfully, ethically and responsibly
   - access and use only ICT facilities, services and information for which they are authorised
   - comply with applicable AIHE policies and procedures and relevant software licence, service and other conditions of use, and
   - comply with reasonable ICT-related directions given by the ICT Manager or other authorised AIHE staff.
5. ICT users must not use AIHE ICT facilities and services to:
   - engage in unlawful, fraudulent, threatening, harassing, discriminatory or otherwise prohibited conduct
   - access, create, store or transmit material, where doing so would breach the law or applicable AIHE policies
   - obtain or attempt to obtain unauthorised access to ICT facilities, services, accounts or information
   - impersonate another user or use another person's account or access credentials without authorisation
   - circumvent or attempt to circumvent ICT security measures or controls
   - introduce, distribute or use malicious software or other tools intended to compromise or disrupt ICT security
   - damage, disrupt or interfere with ICT facilities and services or another person's authorised use of them
   - infringe copyright, intellectual property rights, software licences or other legal or contractual obligations, or
   - use ICT resources in a manner that unreasonably interferes with their availability or performance.
6. AIHE may apply reasonable security controls, access restrictions, usage limits or other measures to ICT facilities and services to support their secure, reliable and efficient operation.

User Accounts and Access Security

7. Access to AIHE ICT facilities, services and information must be authorised through approved AIHE processes and be appropriate to the user's role, responsibilities or study requirements.
8. User accounts and access rights must be created, changed and removed through authorised AIHE processes. Access must be reviewed or adjusted where a user's role, responsibilities, enrolment or other circumstances change, and removed when no longer required.
9. ICT users must:
   - use only accounts and access credentials assigned or authorised for their use
   - keep passwords and other access credentials secure and must not share them with another person
   - comply with authentication and other access security requirements established by AIHE, and
   - promptly report any actual or suspected unauthorised use or compromise of their account or access credentials.
10. ICT users must not attempt to access ICT facilities, services or information beyond the level of access authorised for them.
11. AIHE may restrict, suspend or terminate access to ICT facilities and services where access is no longer required or where this is reasonably necessary to protect ICT facilities, services,

information or users.

Personally Owned Devices

12. A personally owned device used to access AIHE ICT facilities, services or information must be maintained and used in a manner that provides reasonable protection against unauthorised access, loss, malicious software and other security threats.
13. Users of personally owned devices must comply with applicable AIHE security requirements, including requirements relating to device access controls, software and security updates, and the storage or handling of AIHE information.
14. AIHE may refuse, restrict or disconnect access by a personally owned device where the device does not meet applicable security requirements or presents an actual or suspected risk to AIHE ICT facilities, services or information.

Information and Data Security

15. AIHE information must be accessed, stored, processed and transmitted using authorised ICT facilities, services and systems and in accordance with applicable privacy, records management and information security requirements.
16. ICT users must take reasonable steps to protect AIHE information from unauthorised access, use, alteration, loss or disclosure. This includes:
    - accessing AIHE information only where required for authorised work or study purposes
    - taking reasonable precautions to prevent unauthorised persons from viewing or accessing AIHE information
    - ensuring that AIHE information is stored only in authorised locations and services, and
    - taking appropriate care when transmitting or sharing AIHE information.
17. Personal, confidential or otherwise sensitive AIHE information must not be stored on personally owned devices, removable media or external services unless this is authorised and appropriate security protections are in place.
18. ICT users must not deliberately alter, delete, destroy or interfere with AIHE information unless authorised to do so as part of their role or responsibilities.
19. Any actual or suspected loss, unauthorised access, use, alteration or disclosure of AIHE information must be reported promptly in accordance with the incident reporting requirements in this Procedure.

Software, Systems and External Services

20. Software installed or used on AIHE-managed ICT facilities must be appropriately licensed, authorised and compatible with applicable ICT security requirements.
21. ICT users must not install, use or attempt to use software, applications or other tools that:
    - have not been authorised where authorisation is required
    - are unlicensed or used contrary to applicable licence conditions
    - contain or introduce malicious software, or
    - circumvent, disable or otherwise compromise AIHE ICT security controls.
22. Before a new or materially changed ICT system or service is introduced, the officer responsible for the system or service must consider information security, privacy, records management, continuity, legal and contractual requirements, and any risks associated with integration with other AIHE systems.
23. Externally provided or cloud-based services used for AIHE activities must be authorised for that purpose. AIHE information must not be entered into, stored in or shared through an unauthorised external service where doing so could compromise information security, privacy,

records management or other AIHE requirements.

24. ICT users must comply with any conditions or restrictions established by AIHE for the use of particular software, systems or external services. Where an ICT system or service is managed by an area other than ICT, the officer responsible for that system or service must work with the ICT Manager to ensure that applicable ICT and information security requirements are met.

Monitoring and Logging

25. AIHE may generate and retain logs of activity and use of its ICT facilities and services for legitimate operational, security, compliance and investigative purposes.
26. The ICT Manager is responsible for ensuring that ICT logs are monitored and reviewed as reasonably necessary to:
    - maintain the security, availability and performance of ICT facilities and services
    - detect or investigate actual or suspected ICT or information security incidents
    - investigate suspected breaches of AIHE policies, procedures or legal requirements
    - meet legal, regulatory or contractual obligations, and
    - protect AIHE information, assets and operations.
27. An individual ICT user's activity, files, communications or other information may be examined where this is reasonable and necessary for an authorised purpose, including:
    - investigating an actual or suspected security incident or breach of AIHE requirements
    - responding to or recovering from an ICT system failure or other operational incident
    - retrieving AIHE information required for legitimate institutional purposes, or
    - complying with a legal or regulatory requirement.
28. Examination under paragraph 27 must be authorised by the Chief Executive Officer, except where the ICT Manager needs to take immediate action to respond to an ICT or information security threat or system failure. Any such action must be reported to the Chief Executive Officer as soon as practicable.
29. Monitoring and examination of ICT use must be undertaken in a lawful, reasonable and proportionate manner and limited, as far as practicable, to the information necessary for the relevant purpose.

Reporting ICT and Information Security Incidents

30. Staff, students and other authorised ICT users must promptly report any actual or suspected ICT or information security incident to the ICT Service Desk or through any other method specified by AIHE.
31. Incidents that must be reported include, but are not limited to:
    - actual or suspected unauthorised access to an account, system or AIHE information
    - loss, theft or suspected compromise of a device used to access AIHE ICT facilities, services or information
    - loss, unauthorised disclosure or unintended sharing of AIHE information
    - suspected malicious software, phishing or other cyber security threats
    - significant disruption, failure or unusual behaviour affecting ICT facilities or services, and
    - any identified weakness or vulnerability that could reasonably present a security risk.
32. Where an incident presents an immediate or significant risk to AIHE ICT facilities, services, information or operations, it must be escalated promptly to the ICT Manager.
33. A person reporting an incident must provide any information reasonably required to support assessment and response and must not take action that could compromise evidence or impede investigation of the incident.

Responding to ICT and Information Security Incidents

34. The ICT Manager is responsible for coordinating AIHE's response to ICT and information security incidents, in consultation with the Chief Executive Officer and other responsible officers as appropriate.

35. An incident must be assessed as soon as practicable to determine its nature, extent and potential impact. Appropriate action may include:

    - containing or limiting the incident
    - protecting affected ICT facilities, services and information
    - preserving information or evidence relevant to investigation
    - identifying and addressing vulnerabilities or other causes of the incident
    - restoring affected systems, services or information, and
    - seeking specialist or external assistance where required.

36. Where immediate action is reasonably necessary to protect AIHE ICT facilities, services, information or operations, the ICT Manager may temporarily restrict or suspend access, disconnect a device or system, reset or disable access credentials, or take other appropriate protective action. The Chief Executive Officer must be advised as soon as practicable of any significant action taken.

37. Where an incident involves or may involve personal, confidential or otherwise sensitive information, it must be assessed in accordance with the AIHE Privacy Policy and applicable legal and regulatory requirements, including any requirements relating to notification or reporting.

38. Significant ICT and information security incidents must be escalated to the Chief Executive Officer and managed in accordance with AIHE's institutional risk, business continuity or critical incident arrangements, as applicable.

39. AIHE may engage relevant service providers, specialist advisers or external authorities in responding to an incident where this is appropriate or required.

40. Following a significant incident, AIHE will review the incident and its response and identify any reasonable actions required to reduce the likelihood or impact of a recurrence.

Breaches of ICT Requirements

41. An actual or suspected breach of the ICT Policy, this Procedure or applicable ICT requirements must be referred to the ICT Manager for initial assessment.

42. In assessing a suspected breach, the ICT Manager may consult the Chief Executive Officer or other relevant responsible officer and consider the nature, seriousness and potential impact of the matter, including whether it requires further investigation or referral under another AIHE process.

43. Where a suspected breach is minor and does not require referral to a formal conduct process, the ICT Manager may:

    - advise the ICT user of the concern
    - require the user to cease or correct the relevant conduct, and
    - provide or require appropriate guidance or other corrective action.

44. A repeated breach, failure to comply with a reasonable direction, or a matter that may constitute staff or student misconduct must be referred for consideration in accordance with the applicable staff or student conduct process.

45. A suspected breach must not be characterised as misconduct unless this has been determined through the applicable conduct process. Any restriction or suspension of ICT access imposed to

protect AIHE ICT facilities, services, information or operations is a protective measure and does not of itself constitute a finding of misconduct.

46. Matters involving actual or suspected unlawful conduct may be referred to an appropriate external authority where required by law or where otherwise determined appropriate by the Chief Executive Officer.

Backup, Recovery and Disposal

47. AIHE ICT systems and information must be backed up in accordance with arrangements appropriate to their operational importance, sensitivity and recovery requirements.

48. The ICT Manager is responsible for ensuring that appropriate backup and recovery arrangements are maintained for AIHE ICT facilities, services and information. Backup information must be protected against unauthorised access, loss or compromise.

49. Recovery arrangements must be maintained and, where appropriate, tested to support the timely restoration of critical ICT facilities, services and information following disruption, system failure or another significant incident.

50. ICT equipment and storage media that are disposed of, transferred or reused must be managed so that AIHE information is securely removed or rendered irretrievable before the equipment or media leaves AIHE's control or is made available for another purpose.

51. AIHE information must be retained and disposed of in accordance with the AIHE Records Management Policy and other applicable requirements. Decommissioning an ICT system, account, device or service does not of itself authorise the deletion or disposal of AIHE records.

Related Documents

52. Related documents include:
    - AIHE ICT Policy
    - AIHE Privacy Policy
    - AIHE Records Management Policy
    - AIHE Staff Code of Conduct
    - AIHE Student Code of Conduct
    - approved ICT standards, guidelines and related resources.

Definitions

53. Definitions for terms used in this Procedure are contained in the AIHE Glossary of Terms.

Document Control		
Version #	**Date**	**Changes**
1.0	15/12/2017	Procedure approved by General Manager
1.1	17/12/2018	Reviewed; minor edit to clause 1.1
1.2	09/05/2019	Format updated; clause 8.6 added
2.0	17/09/2026	Significant reformatting and editing to better align the Procedure and related Policy and to reflect current ICT and information security requirements.
2.0a	17/09/2026	Procedure approved by Chief Executive Officer

** This Procedure will be reviewed on this date but will be reviewed and updated before this date if circumstances require. If formal review is delayed beyond this date, this Procedure will apply until formal review is possible.*