ICT PROCEDURE

Approving Authority	General Manager	**Approval Date of Last Revision**	09 May 2019
Approval Date	15 Dec 2017	**Effective Date of Last Revision**	09 May 2019
Effective Date	15 Dec 2017	**Review Date***	30 May 2021
Document No	PRO5.1	**Version**	1.2
Parent Policy	ICT Policy		
Policy Category	Operational		
Governing Authority			
Responsible Officer	Manager Student and Academic Services		
Related Documents	ICT Policy Information Technology Acceptable Use Schedule 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 Procedure will still apply beyond the review date.*

Contents

1. PURPOSE

1.1 The Information and Communication Technology (ICT) Procedure supports the principles enunciated in the ICT Policy of Adelaide Institute of Higher Education (AIHE) by:

- establishing clear mechanisms for rapidly responding to any threat to AIHE ICT facilities and services (for instance, via hacking or virus threats);
- providing processes to appropriately handle other security incidents, from minor breaches of Policy through to serious misconduct; and
- clearly delineating the lines of responsibility for managing ICT security incidents within AIHE.

2. SCOPE

2.1 These procedures apply to all users of AIHE ICT facilities and services. It applies to users of AIHE provided devices or bring-your-own-devices.

3. USE OF ICT IN LEARNING AND TEACHING

3.1 The Head of School will ensure Subject and Course Coordinators are aware of and use available technology-based teaching and learning resources in a safe and responsible way, to improve student learning.

3.2 The Head of School will work with the ICT Manager to develop and make available a range of online systems, tools and resources to support digital learning.

3.3 Where ICT is used in learning and teaching, including using ICT as learning, instructional and management tools, AIHE will ensure students and academic staff have timely access to the Learning Management System and have been trained in its use.

4. PERSONAL COMPUTER SECURITY

4.1 To protect the security of AIHE ICT facilities and services:

- AIHE account holders must not allow another person to use their ICT account and password. Similarly, an account holder must not attempt to initiate or operate a computer session by using another person's account and password, or by any other means;
- AIHE account holders must delete any personal files on the public computers or leased computers after use; and
- all AIHE owned or leased personal computers, desktops or laptops must be shut down after use.

5. REPORTING ICT SECURITY ISSUES

5.1 AIHE ICT account holders must report any ICT security issues as follows:

- Report any security weakness or threat to AIHE ICT facilities and services that they suspect or observe to the ICT ServiceDesk by emailing servicedesk@aihe.sa.edu.au;
- Report any known or suspected breaches of the AIHE ICT Acceptable Use Schedule (see Schedule A to the ICT Policy) to the ICT service desk as soon as possible; and
- Report lost, stolen or damaged computers or other ICT equipment to the ICT ServiceDesk as soon as possible. The loss or damage should also be reported to General Manager as an adverse event for insurance purposes.

6. AIHE MONITORING AND LOGGING

6.1 The ICT Manager will ensure that all use of AIHE ICT facilities and services is logged.

6.2 The logs of use will be routinely monitored to assist in the detection of breaches of this Procedure and the ICT Acceptable Use Schedule.

6.3 In addition to routine monitoring, individual account holder's use of ICT facilities will be examined if:

- there is a potential breach of AIHE Policy, or State or Commonwealth Law, is detected or reported, or
- AIHE needs to retrieve or examine the content of electronic documents or messages for purposes such as finding lost files or messages, complying with legal authorities, or recovering from system failure, or
- an account holder's supervisor requests in writing that the account holder's use of ICT facilities, be examined.

6.4 Monitoring the use of AIHE ICT facilities may be undertaken with or without prior notice to the account holder or ICT user.

6.5 AIHE periodically monitors the content of web pages and may request that nominated material be updated or removed.

7. PROCEDURE FOR HANDLING BREACHES OF ICT POLICY THAT CONSTITUTE ILLEGAL ACTIVITY, MISCONDUCT OR SERIOUS MISCONDUCT

7.1 If a breach of ICT policy is detected or reported to ICT Manager that potentially constitutes illegal activity, misconduct or serious misconduct, then the ICT Manager must refer the breach to the General Manager (for staff) or Student Support Officer (for students) who then reports to General Manager.

7.2 The General Manager, ICT Manager and Student Support Officer will:

- assess the material and utilise outside experts or internal expertise as required;
- if emergency suspension of any ICT account is required, authorise the suspension of the account and authorise the impounding of ICT facilities if necessary;
- refer the breach to South Australia Police if required; and
- follow the standard disciplinary or misconduct procedures for any internal treatment of the breach.

7.3 If a breach of the ICT Policy is detected or reported to the ICT Manager that is not potentially illegal, serious misconduct or misconduct:

- the ICT Manager will arrange for an email to be sent to the account holder advising them of the potential breach and asking them to desist from any breaching conduct; and
  - o where the account holder is a staff member, titleholder or visitor, the email will be copied to their supervisor.
  - o where the account holder is a student (unless they are also a staff member or titleholder), the email will be copied to Student Support Officer; and
- if the breaching conduct continues after the first email is sent, then the matter will be treated as potential misconduct and referred under Section 5 above.

8. DATA SECURITY ASSURANCE PROCEDURE

8.1 All staff and visitors with AIHE ICT Accounts will take reasonable steps to assure the security of AIHE data.

8.2 All electronically held AIHE information should be stored in such a way that it is backed up regularly; usually by saving it on a cloud drive that is backed up nightly.

8.3 AIHE ICT facilities that become obsolete must be disposed of in a manner that renders any information illegible and irretrievable at the time of disposal.

8.4 AIHE will manage its ICT facilities in such a way that its ICT facilities and data are protected from:

- unauthorised and unacceptable use;
- wilful, malicious damage or any activity undertaken to purposely bypass security controls on AIHE ICT facilities; and
- virus infection and malicious software.

8.5 AIHE will manage its ICT facilities in such a way that its ICT facilities and data are:

- accurate and complete,
- available to be accessed by authorised ICT users, and only those ICT users, when required, and
- recovered as soon as practicable in the event of serious ICT systems failures or disasters.

8.6 When a student is no longer enrolled in an AIHE course, their access to AIHE learning system and resources will be immediately ceased. The student email and student access to student management system will be maintained for six subsequent months for resolving any issues if any.

9. RESPONSIBILITY FOR THE SECURITY OF ICT FACILITIES

9.1 The ICT Manager is responsible for the physical and technological security of all AIHE ICT facilities and services that it owns, leases or manages on behalf of another area of AIHE.

9.2 The ICT Manager and General Manager are responsible for the security of all ICT facilities owned or leased by their area.

9.3 The security of personally owned computers and ICT equipment used in conjunction with AIHE's ICT facilities is the responsibility of the owner. Owners of this equipment must comply with the security guidelines if the equipment is connected to AIHE's ICT infrastructure.

10. DEFINITIONS

10.1 See the AIHE Glossary of Terms for definitions.

Document Control

Version #	Date	Key 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