Communication and Usage of ICT Policy

Policy Category	Administration
Policy Code	ADM-HE-27
Policy owner	Principal Executive Officer
Responsible Officer	Principal Executive Officer
Approving authority	Board of Directors
Approval date	22 June 2023
Commencement date	29 June 2023
Review date Period	3 years
Version	2023.1
Related documents	Discrimination, Bullying and Harassment Policy Discrimination, Bullying and Harassment Procedure Staff Grievance Policy Staff Grievance Procedure Student Complaint and Appeal Policy Student Complaint and Appeal Procedure Staff Code of Conduct Student Code of Conduct Intellectual Property Policy and Procedure Communication and Usage of Internet and Email Procedure Management of Personal Information Policy Privacy Policy and Procedure SASH Policy and Procedure Records Management Policy and Procedure Telecommunications (Interception and Access) Act 1979 Freedom of Information Act 1982 Cybercrime Act 2001 Copyright Act 1968 Defamation Act 2005 Anti-Terrorism Act 2005 Workplace Surveillance Act 2005 Privacy Act 1988 Discrimination Act 1991
HESF (Threshold Standards) 2021	2.1, 2.3, 2.4, 3.3

1.   Purpose

This Policy sets out the obligations and expectations of students and staff of the Australian Institute of Higher Education ('the Institute') who use the Institute's Information, Communication and Technology (ICT) resources and infrastructure.

2.   Principles

The key principles informing this Policy and associated procedure are:

- All use of the Institute's ICT resources and infrastructure must be compliant with the Institute's policies on Ethical conduct and security of business data.

- ICT resources and infrastructure are provided to assist with day-to-day work and studies at the Institute.
- No person is allowed to use the Institute's ICT resources and infrastructure who has not previously been authorised to do so by the ICT support services staff.
- All users are expected to act in a manner that will not cause damage to ICT resources and infrastructure or disrupt ICT services.

3. Context

This Policy has been developed in order to ensure the ICT resources and infrastructure, including email, computers, internet and all other electronic communications available to Institute staff and students are used in an appropriate and responsible manner.

4. Scope

This Policy applies to all students and staff at the Institute.

5. Definitions

See the AIH Glossary of Terms for definitions.

6. Policy Details

The Institute's ICT resources and infrastructure may only be used by authorised users, and only to carry out the responsibilities of their positions as employees, to further their studies as students, to conduct official business with the Institute, or in other sanctioned activities. Unauthorised access to ICT resources and infrastructure facilities is prohibited and may result in either disciplinary action or criminal prosecution.

6.1 Use of the ICT resources and infrastructure

Use of the ICT resources and infrastructure is encouraged where such use is consistent with the work of students/staff, and with the goals and objectives of the Institute in mind. Reasonable personal use is permissible subject to the following:

Users must adhere to all federal, state and territory laws at all times.

Users must not participate in any behaviours that are likely to bring the Institute into disrepute, or incur liability on the part of the Institute, or adversely impact on the image of the Institute.

Users must not visit, view, download, create, transmit any material which is illegal. This includes, but is not limited to:

- pornography (including child pornography),
- illegal drugs,
- terrorism,
- violence-condoning messages,
- fraud,
- criminal activities,

- race-hate material,

- libel or slander,

- piracy, or

- computer or software viruses.

Users must not visit, view, download, create, transmit any material which is inappropriate to the Institute's business context. This includes, but is not limited to:

- gambling,

- political or religious beliefs and practices,

- social or economic backgrounds, or

- sexual references.

Users must not visit, view, download, create, transmit any material which may reasonably be considered offensive. This includes, but is not limited to:

- obscene material,

- foul language, or

- disparaging comments.

Users must comply with all Institute policy and procedure when using the Institute's ICT resources and infrastructure. Users should carefully review the:

- Discrimination, Bullying and Harassment Policy and Procedure,

- Staff Code of Conduct, Student Code of Conduct,

- Privacy Policy and Procedure,

- Records Management Policy, and

- SASH Policy and Procedure.

These policies and procedures prohibit certain behaviors including, but are not limited to:

- discrimination based on a protected status (age, disability, race, sex, intersex status, gender identity and sexual orientation),

- bullying,

- harassment, and

- sexual harassment.

Personal use of the Institute's ICT resources and infrastructure must not cause an increase for significant resource demand (such as storage, capacity, and speed) or degrade system performance.

Users must not 'hack into' unauthorised areas.

Users must not corrupt or destroy other users' data or disrupt the work of other users.

Users must not waste Staff effort or Institute resources, or engage in activities that serve to deny service to other users.

Users must not be in breach of copyright or license provision with respect to both programs and data, including intellectual property rights

Use of the Internet for personal reasons (such as online banking, shopping, information surfing, social networking) must be limited, reasonable and done only during non-working and non-class time such as breaks.

Staff and students are responsible for all actions relating to any computers or account they use at the Institute, and should therefore make every effort to log off an account or lock the computer when it is not in use ensuring no other person has access without entering their own login details.

Students and Staff are not to share their login information or passwords for the Student Portal, Email or any other logins they may receive from the Institute. It is the responsibility of Students and Staff to protect their login information and passwords.

Users may sometimes need to use the Institute's equipment and access the Institute network while working remotely, whether from home or while travelling. The standards set out in this document apply whether or not Institute equipment and resources are being used.

6.2   Reporting inappropriate activity

Any offensive material received in email must be reported to the ICT Department and Human Resources without undue delay.

Users may face disciplinary action or other sanctions if they breach this Policy and/or bring embarrassment on the Institute or bring it into disrepute.

6.3   Monitoring

All resources of the Institute, including computers, email, and voicemail are provided for legitimate use. If there are occasions where it is deemed necessary to examine data relating to the Institute's ICT resources and infrastructure, then the Institute maintains the right to examine its systems to inspect and review all data recorded in those systems. This examination may occur at any time and without prior notice. The Institute will act in accordance with current legislation in Australia at all times.

Any information stored on a computer, whether the information is contained on a hard drive, USB pen or in any other manner may be subject to scrutiny by the Institute. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists in the management of information systems.

7.   Legislation

All users shall comply with the relevant legislation. This includes the following:

Telecommunications (Interception and Access) Act 1979 / Freedom of Information Act 1982

Any information which the Institute holds may potentially be disclosed to a requester under one of these pieces of legislation. This includes emails.

Users need to be sure that they are not breaching any data protection when they write and send emails. This could include but is not limited to:

- Passing on personal information about an individual or third party without their consent.

- Keeping personal information longer than necessary.

- Sending personal information to a country outside of Australia.

Email should where possible be avoided when transmitting personal data about a third party. Any email containing personal information about an individual may be liable to disclosure to that individual under the Telecommunications (Interception and Access) Act 1979. This includes comment and opinion, as well as factual information. Therefore, this should be borne in mind when writing emails, and when keeping them.

Cybercrime Act 2001

This Act makes it an offence to try and access any computer system for which authorisation has not been given.

Copyright Act 1968

Under this Act it is an offence to copy software without the permission of the owner of the copyright.

Defamation Act 2005

Under this Act it is a civil wrong to publish untrue statements which adversely affect the reputation of a person or group of persons.

Anti-Terrorism Act (No.2) 2005

This Act makes it a criminal offence to encourage terrorism and/or disseminate terrorist publications.

Workplace Surveillance Act 2005

This allows for an organisation to monitor or record communications (telephone, Internet, email and fax) for defined business-related purposes. Any surveillance must be conducted in accordance with the Workplace Surveillance Act 2005.

Privacy Act 1988

The Privacy Act 1988 (Privacy Act) is an Australian law which regulates the handling of personal information about individuals.

8. Version Control

This Policy has been endorsed by the Australian Institute of Higher Education Board of Directors as at June 2023 and is reviewed every 3 years. The Policy is published and available on the Australian Institute of Higher Education website http://www.aih.nsw.edu.au/ under 'Policies and Procedures'.

Change and Version Control				
Version	**Authored by**	**Brief Description of the changes**	**Date Approved:**	**Effective Date:**
2017.1	Ms. McCoy	Moved procedure to separate document	1 March 2017	6 March 2017
2020.1	CEO	Reviewed and updated	2 December 2020	3 December 2020
2022.1	Registrar	Updated Higher Education Standards Framework [Threshold Standard] 2021	25 May 2022	26 May 2022
2023.1	Registrar	Major review and rewrite of policy with name change	22 June 2023	29 June 2023