AUSTRALIAN INSTITUTE
OF HIGHER EDUCATION

Communication and Usage of ICT Procedure

Policy supported	Communication and Usage of ICT Policy
Policy Code	ADM-HE-27
Owner	Principal Executive Officer
Responsible Officer	Systems Manager
Approving authority	Board of Directors
Approval date	2 June 2023
Commencement date	29 June 2023
Review date	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 Procedure supports the Communication and Usage of ICT Policy, which 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. Scope

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

3. Definitions

See the AIH Glossary of Terms for definitions.

4. Actions and Responsibilities

4.1 General Responsibilities

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. Care should be taken that staff and students take reasonable steps to ensure the security of their account(s) and the information accessible to them. This includes, but is not limited to:

- ensuring screens are not unnecessarily exposed to unauthorised users
- following prompts to set and update strong (14+ character) passwords in a secure manner,
- maintaining appropriate version control,
- secure storage of passwords and other account security information
- storing Institute devices safely and securely, particularly during travel.

Any accidental damage or disruption caused by staff or students must be reported to IT support services as soon as possible after the incident has occurred.

4.2 Using the Institution Email

Students must ensure that use of the Institute's email account provided for student use complies with the Google program policy. See https://www.google.com/intl/en/mail/help/program_policies.html for further details.

The student email account is provided so that Institute staff may communicate with students about administrative matters and to facilitate communication with lecturers and fellow students. Note that students are advised to limit personal use of an Institute email account.

The staff email account is provided so that Institute staff may communicate with students and staff as part of their role. Care should be taken to only use the Institute account when conducting Institute business. Emails sent from an Institute domain may be interpreted by others as Institute statements. Staff should carefully consider their use to ensure the Staff Code of Conduct is adhered to at all times.

Users should delete all personal emails and attachments when they have been read and should also delete all unsolicited junk mail. In the process of archiving emails, users should ensure inappropriate material is not archived.

4.3 Good Practice

Confidentiality

Where sensitive and confidential information needs to be sent electronically for practical reasons, please be aware that email and some communication applications are essentially a non-confidential means of communication. Emails and messages can easily be forwarded or archived without the original sender's knowledge. They may be read by persons other than those they are intended for.

Content and Tone

Users must exercise due care when communicating online to avoid being rude or unnecessarily terse. Users are responsible for ensuring that their content and tone is appropriate. Online communication may need to be as formal and business-like as other forms of written correspondence. It is best to avoid using styles, formatting or symbols that can be used to convey intense emotion such as Caps Lock, multiple exclamation marks or red highlighting.

Standard Tone should be used so that communication is as clear as possible while retaining accuracy.

Viruses and Scams

The Institute is aware of the threat that viruses and scams are to individuals and businesses. The Institute provides a current and up to date automatic virus checker on all networked computers. However, caution should be used when opening any attachments or emails, downloading data, or visiting sites online. Users should exercise caution in the following ways:

- Consider any unusual messages carefully. Scammers often inject a sense of urgency to any communication to stop the user from thinking carefully before acting. This urgency can arise from a threat to your Student Visa, employment or from a government agency threatening legal action such as the Police or Tax Office.
- Check that the message is real. Rather than replying to a message using links or forums provided by the message, search for the publicly available phone number or email address. If the message originates from a staff member, ask them to confirm the contents in another method of communication, e.g. Moodle, through Student Services or in person. Errors in spelling and grammar are often present in scams.
- Be aware of key announcements and dates. Due dates for fees, self-enrolment and other deadlines are often announced in advance and in multiple locations.
- Ensure that you use reliable sources for downloading of material such as official websites and software. The Institute supplies student licenses for common software and you can ask your lecturer for recommendations of reliable open-source software.
- Install a virus checker on your devices. The Institute's devices have virus checkers already installed. It is a disciplinary offence to disable the virus checker.

4.4 Monitoring

Monitoring will be undertaken by authorised Staff only and in accordance with the Institute's Management of Personal Information Policy.

4.5 Reporting and Investigating Improper Use

Staff

Staff must report improper use of any Institute ICT resources and infrastructure in accordance with the Staff Grievance Policy and associated procedures. Questions and assistance can be sought from the Systems Manager.

Any staff member alleged to have misused any Institute ICT resources and infrastructure will be investigated in accordance with the **Staff Code of Conduct**.

Students

Students and staff who receive improper email from individuals inside or outside the Institute should discuss the matter in the first instance with the Institute's IT Support Service (assist@celoxgroup.com.au) Students can report improper use of the internet and email in accordance with the Student Complaint and Appeal Policy and associated procedures.

Any student alleged to have misused the internet or email will be investigated in accordance with the **Student Code of Conduct**.

4.6 Penalties for Improper Use

Breaches of this Policy or Procedure may be dealt with under the Institute's disciplinary procedures. Users in breach of these regulations may have access to the Institute's IT facilities restricted or withdrawn.

Where a staff member has breached this Policy or Procedure, it may lead to termination of employment from the Institute. The breach of code of conduct procedure outlined in the **Staff Code of Conduct** will be followed.

Where a student has breached this Policy or Procedure, the misconduct procedures outlined in the **Student Code of Conduct** will be followed.

Breaches of the Law

Where appropriate, breaches of the law will be reported to the relevant external law enforcement agencies. Individuals may be subject to prosecution.

5. Version Control

This Procedure has been approved by the Australian Institute of Higher Education Board of Directors as at June 2023 and is reviewed every 3 years. The Procedure 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:
2016-2	Registrar	Drafted document from policy doc	6 July 2016	6 August 2016
2017-1	Ms. McCoy	Revised content.	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	Compliance and Executive Officer	Changed name to be consistent with Policy name change. Formatting updates. Inclusion of additional relevant documents in top table. Broadened and modernized advice in section 4. Addition of detail to Viruses and Scams. Included contact details for reporting purposes. Approving authority corrected from CEO to Board of Directors	2 June 2023	29 June 2023