AUSTRALIAN INSTITUTE
OF HIGHER EDUCATION

Communication and Usage of Internet and Email Policy

Policy Category	Administration
Policy Code	ADM-HE-27
Policy owner	Chief Executive Officer
Responsible Officer	Chief Executive Officer
Approving authority	Board of Directors
Contact Officer	Registrar
Approval date	1 March 2017
Commencement date	6 March 2017
Review date	3 years
Version	2017.1
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 Communication and Usage of Internet and Email Procedure Management of Personal Information Policy 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

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 IT facilities for Internet and email purposes.

2. Principles

The key principles informing this Policy are:

- that, while IT facilities are provided to assist with day to day work and studies, it is important that they are used responsibly, are not abused, and that individuals understand the legal professional and ethical obligations that apply to them;
- that no person is allowed to use the Institute's IT facilities who has not previously been authorised to do so by the IT support services staff; and

- that all users are expected to act in a manner that will not cause damage to IT facilities or disrupt IT services.

3. Context

This Policy has been developed in order to ensure the IT services available to Institute staff and students are used in an appropriate and responsible manner.

4. Scope

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

5. Definitions

See the ***AIH Glossary of Terms*** for definitions.

6. Policy Details

The Institute's IT resources may only be used by authorised users, and only to discharge 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 IT facilities is prohibited and may result in either disciplinary action or criminal prosecution.

6.1 Use of the Internet

Use of the Internet 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 not participate in any online activities that are likely to bring the Institute into disrepute, create or transmit material that might be defamatory or incur liability on the part of the Institute, or adversely impact on the image of the Institute.
- Users must not visit, view or download any material from an Internet site which contains illegal or inappropriate material. This includes, but is not limited to, pornography (including child pornography), obscene matter, race hate material, violence condoning messages, criminal skills, terrorism, cults, gambling, and illegal drugs.
- Users must not knowingly introduce any form of computer virus into the Institute's computer network.
- Personal use of the Internet 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 download commercial software or any copyrighted materials belonging to third parties, unless such downloads are covered or permitted under a commercial agreement or other such licence.
- Users must not use the Internet for personal financial gain.
- Users must not use the Internet for illegal or criminal activities, such as, but not limited to, software and music piracy, terrorism, fraud, or the sale of illegal drugs.
- Users must not use the Internet to send offensive or harassing material to other users.

- 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-class time such as breaks.

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.

6.2 Use of Email

Staff and students are responsible for all actions relating to their email account/pc username, and should therefore make every effort to ensure no other person has access to their account.

When using the Institute email, users must:

- ensure they do not disrupt the Institute's wider IT systems or cause an increase for significant resource demand in storage, capacity, speed or system performance e.g. by sending large attachment to a large number of internal recipients.
- ensure they do not harm the Institute's reputation, bring it into disrepute, incur liability on the part of the Institute, or adversely impact on its image.
- not seek to gain access to restricted areas of the network. "Hacking activity" is strictly forbidden
- must not use email for the creation, retention or distribution of disruptive or offensive messages, images, materials or software that include offensive or abusive comments about ethnicity or nationality, gender, disabilities, age, sexual orientation, appearance, religious beliefs and practices, political beliefs or social background. Students who receive emails with this content from other students of the Institute should report the matter to the Executive Dean or IT support Staff.
- not send email messages that might reasonably be considered by recipients to be bullying, harassing, abusive, malicious, discriminatory, defamatory, and libellous or contain illegal or offensive material, or foul language.
- not upload, download, use, retain, distribute, or disseminate any images, text, materials, or software which might reasonably be considered indecent, obscene, pornographic, or illegal.
- not engage in any activity that is likely to
    - Corrupt or destroy other users' data or disrupt the work of other users
    - Waste Staff effort or Institute resources, or engage in activities that serve to deny service to other users
    - Be outside of the scope of normal study-related activities – for example, unauthorised selling/advertising of goods and services
    - Affect or have the potential to affect the performance or damage or overload the Institute's system, network, and/or external communications in any way
    - Be a breach of copyright or license provision with respect to both programs and data, including intellectual property rights
- not send chain letters or joke emails from an Institute account.

6.2 Passwords and Login Information

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. Students and staff must make sure they log off computers that they are no longer using and when away from the computer, ensure the screen is locked.

6.3 Remote Users

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.

6.4 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 beyond that of the normal business activity of the Institute then, at any time and without prior notice, the Institute maintains the right, subject and in accordance with current legislation in Australia, to examine any systems and inspect and review all data recorded in those systems.

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:

7.1 *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.

7.2 *Cybercrime Act 2001*

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

7.3 *Copyright Act 1968*

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

7.4 *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.

7.5 *Anti-Terrorism Act 2005*

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

7.6 *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*.

7.7 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 Australia Institute of Higher Education Board of Directors as at March 2017 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