

Acceptable Use of Information and Communications Technology Policy



Purpose/objective

This Policy provides the framework that governs the acceptable use of AAHE's enterprise information and communications technology (ICT). It is intended to ensure that AAHE's ICT systems and resources are:

- protected against accidental or malicious misapplication, unauthorised access or disclosure, modification, corruption, or destruction
- used appropriately and ethically for their intended purpose
- comply with applicable laws governing information management and security.

This Policy should be read in conjunction with the Information and Communications Technology Provisioning Policy and the Information and Communications Technology Security Policy.

The Acceptable Use of Information and Communications Technology Procedure explains how this Policy is implemented.

Scope

This Policy and Procedure applies to:

- all AAHE staff and students, contractors, visitors and any other parties that have access to AAHE's ICT systems, resources and networks
- ICT systems and resources owned, leased or operated by AAHE or third parties on behalf of AAHE

Definitions

Terms used in this document are defined in the AAHE Glossary.

Policy

1. Key principles

- 1.1 AAHE is committed to providing its students with the latest ICT systems and resources that support their learning and their engagement with fellow students, staff and AAHE's administrative processes.
- 1.2 The ICT systems and resources are strategic assets that AAHE relies on for the purposes of learning, teaching, scholarship and all administrative and business-related functions and operations.
- 1.3 Every person associated with AAHE has a role to play in protecting the organisation from information security risks and must become familiar and comply with this policy when engaging in activities that use AAHE's ICT systems and resources.
- 1.4 AAHE will provide its students, staff and affiliates with ICT resources that are fit for purpose, accessible, reliable and promote innovation and creativity.
- 1.5 All students shall be provided equitable access to ICT systems and resources in accordance with AAHE's Equity and Diversity Policy and Procedures.

1.6 AAHE's ICT systems and resources must comply with the relevant standards in the Higher Education Standards Framework (Threshold Standards) 2021 and relevant legislation.

2. General use and access

2.1 Only authorised persons may use AAHE's ICT systems and resources on legitimate AAHE business and only to the extent required to carry out activities that relate to their duties and role.

2.2 Unauthorised access is prohibited by law under the *Cybercrime Act 2001* and may result in disciplinary action and/or criminal prosecution.

2.3 All users of AAHE's ICT systems and resources have an obligation to behave professionally, responsibly, ethically, lawfully, and with respect for the rights and privacy of others.

2.4 Users must take reasonable steps to protect their AAHE ICT user accounts and privileges from unauthorised use.

2.5 Use of AAHE ICT resources or Bring Your Own Devices (BYOD) that students or staff connect to AAHE ICT infrastructure must not jeopardise the security, reliability, productivity or integrity of the ICT environment and the business operations, data and information management it supports.

2.6 AAHE will monitor and audit the use of AAHE's ICT systems and resources to ensure they are used in an efficient, effective and secure manner.

2.7 Information stored on AAHE's ICT systems, whether owned or leased by AAHE, remains the sole property of AAHE.

2.8 All information, metadata, data or files created, downloaded or stored by users while employed or enrolled at AAHE can be monitored and subject to investigation. All electronic messages are official documents, subject to the same laws as any other form of correspondence. They are subject to statutory record keeping requirements and can be subpoenaed during legal processes.

2.9 AAHE reserves the right to record, delete, block, quarantine, copy, use and take possession of all ICT systems, and any communications or data they hold, and pass on the information to external organisations where legally obliged to do so or in cases of possible breaches of AAHE policies or procedures.

3. Use of Internet and Email

3.1 Users are not permitted to use AAHE's internet or email for the following purposes:

- criminal or illegal activities
- transmitting material which could be deemed fraudulent, defamatory, profane, offensive, discriminatory, or harassing
- making comments or using images, materials or software that might be considered offensive or abusive under Anti-Discrimination legislation and codes
- viewing, downloading, transmitting or retaining illegal, obscene, pornographic or otherwise inappropriate material
- sending mass messages of a commercial, political, lobbying or fundraising nature
- sending, receiving or storing any copyright infringing works
- disclosing private, sensitive or confidential information of a personal or organisational nature, unless required by law
- sending or soliciting chain letters or spam
- gambling, or
- unauthorised access to restricted areas of the network.

- 3.2 In addition, users must not:
- maliciously interfere with AAHE’s ICT resources, network, or network infrastructure
 - compromise AAHE’s reputation
 - access the email account of a student or staff member unless officially authorised to do so for legitimate purposes by the COO, or
 - place AAHE in a position where liability is incurred.
- 3.3 Personal use of the Internet, email and social media is only sanctioned where it complies with sections 3.1 and 3.2 (above), and where such use is strictly limited, does not impede professional duties or disrupt others, and does not place an undue burden on network resources.

Related documents and relevant legislation

Business Continuity Management Policy and Procedure

Cyber Incident Response Plan

Delegation of Authority Policy and Schedule

Equity and Diversity Policy and Procedure

[Higher Education Standards Framework \(Threshold Standards\) 2021](#)

Information and Communications Technology Security Policy and Procedure

Information Management and Security Policy and Procedure

Intellectual Property Policy and Procedure

Privacy Policy and Procedure

Records Management Policy and Procedure

Resources and Infrastructure Plan

Risk Management Policy, Plan and Measurement

Sexual Assault and Sexual Harassment Policy and Procedure

Student Code of Conduct

Staff Code of Conduct

Document information

Document owner: Board of Directors

Version	Approved by	Approved on	Implementation date	Changes made
1	Board of Directors	16/9/21	1/10/23	

Acceptable Use of Information and Communications Technology Procedure

1. General use and access

- 1.1 Authorisation to use AAHE ICT resources will be given to staff upon commencement of employment with AAHE and to students upon enrolment into a course of study.
- 1.2 Only authorised persons may use AAHE's ICT resources. It is an offence under the *Cybercrime Act 2001* to access or attempt to access any computer system for which due authorisation has not first been obtained. Unauthorised access is prohibited by law and may result in disciplinary action and/or criminal prosecution.
- 1.3 Authorisation may be granted to contractors and other third parties for purposes that may be deemed necessary by the Chief Operating Officer.
- 1.4 Rights to use AAHE ICT resources are non-transferrable, unless authorised by the Chief Operating Officer.
- 1.5 Access to ICT resources will cease at the end of a person's relationship with AAHE (eg upon graduation or cessation of employment).
- 1.6 Users of AAHE's ICT systems and resources have a responsibility to ensure they do not:
 - breach copyright or license provision, or copy software without the express permission of the copyright owner
 - disrupt, corrupt or destroy the work of others
 - adversely affect, damage, destroy, or place an undue burden on AAHE's ICT systems, resources, network and/or network infrastructure, or
 - knowingly misuse or waste ICT resources.
- 1.7 AAHE is responsible for ensuring users are provided with a reliable and robust network service. To this end, AAHE will:
 - provide sufficient training in ICT services and skills
 - ensure equitable access to learning technologies, the Internet and email
 - ensure students are not disadvantaged in the event of unscheduled outages, and
 - develop and implement appropriate risk management processes to minimise service disruption or outages.
- 1.8 Under the Workplace Surveillance Act 2005, AAHE may monitor or record ICT systems usage and digital communications for defined business-related purposes.
- 1.9 In the interests of ensuring compliance with this policy and procedure and related legislation, AAHE reserves the right to undertake the following without notice:
 - inspect, investigate, suspend, and/or terminate all user accounts from AAHE ICT systems and resources
 - block, inspect, redirect or reject any online activities or emails
 - remove or delete any Internet resources; and
 - monitor Internet activity.
- 1.10 Users of AAHE ICT facilities and resources have a responsibility to promptly report to the IT/LMS Officer:
 - any potential or actual damage or disruption to AAHE's ICT systems or resources
 - the theft, loss or unauthorised disclosure of AAHE proprietary information and any behaviour that falls under section 1.6 above.

2. Use of internet and email

- 2.1 Users of AAHE’s ICT systems and resources have a responsibility to:
- protect the privacy of their email accounts, and safeguard passwords
 - change passwords regularly
 - ensure they are using secure and approved technologies, including antivirus software
 - be careful when opening attachments or emails from unknown or unidentifiable senders
 - respect confidentiality and handle sensitive information accordingly
 - delete all personal emails and attachments once read
 - delete all unsolicited junk mail
 - ensure the content and tone of emails are appropriate and courteous
 - ensure any comment made in a private and personal capacity is explicitly designated as such
 - observe all relevant legislation, standards and codes, and
 - bring any concern with respect to the Internet, email or social media to the attention of the IT/LMS Officer as promptly as possible.
- 2.2 AAHE reserves the right to monitor both usage and content of email messages, instant messages, discussion forums and visits to Internet sites using AAHE resources to:
- identify inappropriate use
 - protect system security
 - maintain system performance
 - protect the rights and property of AAHE
 - determine compliance with policy and state and Commonwealth laws.
- 2.3 AAHE also monitors and records network traffic including:
- email and internet sites accessed
 - usage data such as account names, source and destination accounts and sites
 - user location data
 - dates and times of transmission or access
 - size of transmitted material
 - other usage related data such as utilisation of wireless access points.
- 2.4 This information is used for accounting purposes, troubleshooting, systems management, analytics, user personalisation, and meeting legal and compliance obligations.

Document information

Document owner: Chief Operating Officer

Version	Approved by	Approved on	Implementation date	Changes made
1	Board of Directors	16/9/21	1/10/23	