

IT Acceptable Use Policy

Version 1.0

Overview

The purpose of this policy is to ensure the appropriate, secure, and responsible use of information technology resources at AIM Institute.

This policy protects the Institute's information systems, data, and digital infrastructure while supporting teaching, learning, research, and administrative operations.

Scope

This policy applies to:

- all employees, contractors and consultants
- all students enrolled at AIM Institute
- third-party users authorised to access Institute systems.

It applies to the use of:

- computers and mobile devices provided by AIM Institute
- learning management systems (LMS)
- student management systems
- email systems
- cloud storage and collaboration platforms
- internet access provided by the Institute
- any other digital system owned, managed, or licensed by AIM Institute.

Policy and Procedure

Policy Principles

AIM Institute provides information technology resources to support education, research, administration, and communication.

Users must use these resources responsibly, ethically, and in compliance with applicable laws, institutional policies, and cyber security requirements.

Improper use of IT resources may expose the Institute to security risks, legal liability, or reputational damage.

Acceptable Use

Users may use AIM Institute IT systems for legitimate educational and work-related purposes, including:

- teaching and learning activities
- academic research
- administrative functions
- communication with students, staff, and external stakeholders
- access to authorised online learning platforms and academic resources.

Limited personal use may be permitted provided it:

- does not interfere with work or study obligations
- does not compromise system security
- does not incur significant cost to the Institute.

Prohibited Use

Users must not use AIM Institute IT resources to:

- access, store, or distribute illegal material
- engage in harassment, bullying, discrimination, or offensive conduct
- transmit malicious software or intentionally introduce security risks
- attempt to gain unauthorised access to systems or data
- share login credentials with other users
- download or distribute copyrighted material unlawfully
- install unauthorised software on Institute devices
- use systems for personal commercial activities without approval.

Account Security

Users are responsible for maintaining the security of their accounts and passwords.

Users must:

- keep passwords confidential
- use strong passwords
- log out of shared devices
- report suspected compromised accounts immediately
- follow multi-factor authentication requirements where implemented.

Email and Communication

AIM Institute email systems must be used responsibly.

Users must not:

- send spam or unsolicited bulk messages
- send fraudulent or misleading communications
- distribute offensive or inappropriate content

- impersonate other individuals.

Users must exercise caution when opening email attachments or clicking external links.

Data Protection and Privacy

Users must protect confidential and personal information including:

- student records
- staff information
- academic materials
- financial information.

Users must:

- access only information necessary for their role
- store sensitive information securely
- comply with the Privacy Act 1988 and AIM Institute privacy policies.

Device and Network Use

Institute-owned devices must be used responsibly.

Users must:

- not disable security controls
- keep devices updated where possible
- secure devices when unattended
- report lost or stolen devices immediately.

Access to the Institute network may be monitored to protect system security.

Monitoring and Privacy

AIM Institute reserves the right to monitor the use of its IT systems in order to:

- protect system security
- investigate potential policy breaches
- ensure compliance with legal and regulatory obligations.

Monitoring will be conducted in accordance with applicable privacy legislation.

Reporting Security Incidents

Users must report any suspected cyber security incidents immediately, including:

- suspicious emails or phishing attempts
- unauthorised system access
- malware alerts
- lost or stolen devices.

Incidents should be reported to the IT Manager or Compliance Manager.

Breach of Policy

Failure to comply with this policy may result in:

- suspension of system access
- disciplinary action for staff
- student misconduct proceedings
- possible legal or regulatory action.

Related Policies

Review

This policy will be reviewed every two years or earlier if required due to regulatory or technological changes.

Related Legislation	The Higher Education Standards Framework (Threshold Standards) 2021 Tertiary Education Quality and Standards Agency (TEQSA) Act 2011 Privacy Act 1988 (Cth)
Related Policies and Statements	Cyber Security and Cyber Incident Response Policy Privacy Policy Records Management Policy Student Code of Conduct Staff Code of Conduct.

Document Approval

Endorsed by:	Board of Directors		
Date endorsed:	24/03/2026		
Effective date:	24/03/2026		
Version number:	1.0		
Last amendment date/by:	7/04/2026,		
Review due date:	24/03/2028		
Alignment to HESF	2.1 Facilities and Infrastructure	3.3 Learning Resources and Ed.Support	Choose an item.
Responsibilities:			

Contact:	info@aiminstitute.nsw.edu.au +61 02 4505 1924
-----------------	--

Document Change and Review log

Version	Updated by	Approval date and body	Details
1.0	TWEIR	Choose an item.	