INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

Category	Communications and ICT
Policy Owner	Chief Technology Officer
Last review	15 September 2025
Next review	30 September 2026
Approved by	Vice-Chancellor
Effective date	2 February 2024

1. PURPOSE

The purpose of this policy is to ensure that AUT's ICT Systems & Services are well managed and secure and that Users of AUT's ICT Systems & Services understand the rules that govern their use of those systems.

AUT is committed to protecting the confidentiality, integrity and availability of Information entrusted to it by staff, students, and its partners, and to maintaining the balance between user experience and the management of business and user risk.

This policy therefore aims to ensure that AUT's ICT Systems, services, Software, and other ICT Assets are selected, managed, and used appropriately.

This policy:

- Ensures that all Users are aware of AUT's arrangements for managing and maintaining the security of its ICT Systems & Services;
- Describes acceptable and unacceptable use of the ICT Systems & Services; and
- Describes the responsibilities each user has for maintaining security when using the ICT systems.

2. POLICY

Principles

- AUT makes approved ICT Systems & Services available to authorised Users for the purpose of supporting teaching, learning, research, and administration.
- ICT Systems & Services play a critical role in University operations and support the achievement of strategic goals and initiatives.
- Data and Information are a strategic University asset, they are protected, and their quality and Integrity are maintained throughout their lifecycle. Data and Information will be well defined, discoverable, and reusable.
- Mātauranga Māori and te reo Māori are taonga unique to Aotearoa New Zealand and as such should be protected and meaningfully incorporated into every part of the University in partnership with Māori for the benefit of all. ICT Systems & Services should increase respect and safe access to Mātauranga Māori and te reo Māori while ensuring its use is culturally affirming and mana enhancing for everyone.

- Data collected about Māori members of the AUT community, or research that concerns Māori communities and knowledge, is subject to Māori data sovereignty and must be managed, stored, and analysed in ways that respect Māori cultural values and rights.
- All Users are collectively responsible for the security and protection of the University's ICT Systems & Services and Information.
- The University will deliver meaningful management Information from agreed data sources, eliminating multiple versions of the same data.
- Collaboration and innovation through Information technology is encouraged.

Application of this Policy

ICT Services will investigate reported or suspected policy breaches.

Breach of the policy may have consequences for the user. The consequences of any breach will depend upon the breach and the nature of the user's relationship with AUT but may include termination of contract, termination of employment or termination of access to ICT systems.

The application of this policy to any person does not change the nature of the relationship between AUT and such person and, in particular, does not create an employment relationship.

This policy does not form any part of any person's terms of employment or engagement with AUT.

AUT may amend, or revoke this policy, or any part of it, at any time.

User Responsibilities

All Users will at all times act in a responsible, professional, security-aware manner with respect to their use of AUT's ICT Systems and Services, including by:

- Complying with all legal and contractual obligations;
- Protecting the confidentiality, integrity, and availability of AUT's ICT Systems & Services, and Information at all times;
- Taking all reasonable steps to ensure physical protection of AUT's computer facilities;
- Immediately reporting full details of breaches or identified vulnerabilities in the security of any ICT Systems & Services to ICT Services;
- Reporting any other identified security improvements to ICT Services;
- Ensuring their passwords are not disclosed or used by others;
- Using ICT Systems and Software for legitimate purposes only and not any use that is considered by AUT to be unacceptable, which includes those activities listed below;
- Complying with all controls, rules and requirements established by ICT Services and
- Ensuring private, sensitive, or very sensitive Information is not accessed, or disclosed to anyone, without permission.

Acceptable Use

The types of activities that Users are encouraged to participate in and considered acceptable practice when using ICT systems include:

- Teaching, learning, research and administration;

- Coursework and associated activities, including accessing course and lecture notes and recordings;
- Acquiring or sharing Information necessary or related to the performance of your assigned responsibilities or course; and
- Reasonable use of ICT systems for personal use, e.g., sending personal emails and using internet web sites so long as it does not interfere with productivity, require installation of additional Software, or consume sustained high-volume traffic.

Unacceptable Use

The types of activities that are considered unacceptable include, but are not limited to:

- Use of ICT systems for illegal or unlawful purposes. This includes, but is not limited to:
  - Copyright infringements;
  - Plagiarism;
  - Software license infringements;
  - Fraud;
  - Forgery;
  - Hoax calls;
  - Hacking; and
  - Other computer tampering (e.g., spreading computer viruses or destruction of data owned by others).
- Use of ICT systems for improper purposes relating to coursework, including but not limited to the use of any Software that breaches AUT's Academic Integrity Guidelines and Procedures.
- Use of ICT systems to access internet sites or receive or disseminate Information with the effect or intention of causing harm, damage or other detriment of any kind to any other person, organisation, or AUT including, but not limited to:
  - Bullying;
  - Intimidation;
  - Harassment;
  - Defamation
  - Impersonation;
  - Misinformation/Disinformation
  - Discrimination or hate speech;
  - Mobbing;
  - Obscenity; and
  - Pornography.
- Failing to comply immediately with and ICT Services instruction to cease using or remove and Software, program, application or Hardware.
- Bypassing or disabling controls on any ICT Assets or ICT Systems & Services.
- Obfuscation of any network activity or usage of ICT Systems & Services.
- Attempting to gain access to any computer system, Information, or resources without the authorisation of the relevant owner.
- Disclosing or sharing any password or restricted access to any aspect of the ICT systems, including being reckless, negligent, or otherwise failing to take adequate steps to protect against disclosing or sharing any password or ICT system access.
- Knowingly or recklessly transmitting or distributing any Information or material which contains a virus, worm, Trojan Horse, or any other harmful component.

- Creating, developing, installing, or using any partition, firewall, encryption, password protection or other security measure of any kind that has not been approved by ICT Services.
- Disabling or attempting to disable (whether temporarily or permanently) any security or other protection.
- Posting, publishing, transmitting, or distributing any unsolicited advertising through mass email or other direct transmission.
- Use of ICT Systems & Services, and internet services to reveal or publicise restricted, confidential, or proprietary Information, which includes, but is not limited to, financial Information, intellectual property, strategies and plans, databases and the Information contained therein, staff, student or user details, computer Software and code, computer network and access details and business relationships.
- Internet use of a nature that is deemed unacceptable by ICT Services, e.g. usage that interferes with provision of other ICT Systems & Services.
- Failing to comply immediately with any ICT Services instruction to cease the unacceptable internet use.
- Making any material available in the public domain that could damage the reputation of the University (not being Information to which the Protected Disclosures Act 2000 relates);
- Unauthorised use, access, alteration, damage, disclosure, duplication, diversion, destruction, or removal of University Information or facilities;
- Unauthorised access to, communication of or storage of unacceptable or offensive material including pornography or language that is abusive or insensitive to matters such as race, ethnicity, sex, sexual orientation, disability or religion;
- Illegal, fraudulent activity or any other activity which in the opinion of the University, breaches or contravenes this policy;
- Any wilful activity that may interfere with the Confidentiality, Integrity or Availability of the University's ICT Systems and services;
- Masquerading as another User, use of remote access, Shadowing technologies or Spyware to intrude on the work or privacy of a User unless one of the following conditions is met: Approval is given by the Vice Chancellor or their delegated authority or it is done with the knowledge and specific consent of the User.

Prompt action will be taken to deal with unacceptable actions by any user who breaches this policy or whose acts or omissions undermine or have the potential to undermine the integrity or performance of any ICT system or service.

The consequences of any breach will depend upon the nature of the user's relationship with AUT but may include termination of contract, termination of employment or termination of access to ITC systems.

Systems and Services

AUT manages the evaluation, acquisition, development, integration, installation and lifecycle of all ICT Systems & Services. ICT Services will partner with business units in this management and will make recommendations and decisions to ensure alignment with the University's strategic objectives for ICT.

ICT Systems & Services:

- Only approved Software is to be installed on AUT's ICT systems. Advice on approved Software is available from ICT Services;

- Non-approved Software that is installed will not be supported by ICT Services and may be removed;
- Users must not remove copy protection from any Software;
- All Software must be licensed for use and used only within the terms of that licensing;
- No Software is to be installed when there are insufficient licenses available; and
- ICT Services will register and manage all website domain addresses and website certificates on behalf of AUT.
- ICT Services will maintain registers of managed ICT Systems & Services.

Hardware and ICT Assets

ICT Assets should be managed throughout their lifecycle to ensure they remain operational, well maintained, and secure. The following apply:

- Hardware and ICT Assets remain the property of AUT, even if specifically issued to a particular user and must be returned immediately on request at any time;
- ICT Services is authorised to install and configure Software and make configuration changes to ICT systems;
- Hardware, Software, or ICT Services purchasing must be in accordance with the Procurement Policy and Procedures;
- All ICT Assets are required to be recorded by ICT Services and physical assets will be identified with a unique asset number;
- This number is to remain visible and only the ICT Services is permitted to remove the asset identifier;
- Users may not deliberately cause any harm or damage to any ICT Asset or Hardware or act (or omit to act) in any way that is likely to cause such harm or damage;
- In the event of any ICT Asset or Hardware being lost, damaged (accidentally, negligently, or deliberately) or stolen the incident is to be reported to ICT Services immediately;
- All removable media, (for example: disks, USBs, portable/external drives, laptops, tablets, phones) that contain confidential or above material are to be stored overnight in a locked cabinet, locked drawer/room or a locked fireproof safe;
- All removable media must be encrypted to reduce the risk of data being compromised in the event of it being misplaced or stolen. All Users must follow ICT Services instructions in this respect;
- Only ICT Services are authorised to dispose of Hardware and ICT Assets; and
- All Hardware and ICT Assets will be securely wiped of data before disposal.

Social Media

All use of social media using AUT's ICT systems must comply with the Social Media Policy and the responsibilities and rules regarding acceptable and unacceptable use set out above.

Only Users with specific approval from AUT may purport to make any public statement, including on social media, on behalf of AUT.

ICT Services may monitor all use of social media using ICT systems and therefore each user acknowledges that there is no expectation of privacy,

Privacy

AUT is the owner of and ultimately responsible for the ICT Systems & Services.

AUT will comply with the Privacy Act 2020 and its Privacy Policy in relation to personal Information contained in ICT Systems & Services.

Users should be aware that their use of ICT Systems & Services may be monitored, and their personal Information accessed as set out in the Privacy Policy.

3. DEFINITIONS

Hardware: The physical components of all technologies used for the capture, storage, retrieval, processing, display, representation, organization, management, security, transfer, and interchange of data and Information.

ICT: Information and communication technology.

ICT Assets: AUT's Information & communication technology Hardware. [owned or approved]

ICT Services: The Office of Information & Communication Technology Services at AUT.

ICT Systems & Services: encompasses all AUT's ICT for the capture, storage, retrieval, processing, display, representation, organisation, management, security, transfer, and interchange of electronic data and Information and includes, for the avoidance of doubt, all AUT's Hardware, Software, applications and internet facilities.

Information: all records, documents, and data (whether computerised or not) and all Software (whether developed by AUT or otherwise acquired,) that is owned by AUT or licensed, given or entrusted to it for any purpose or used during or associated in any way with AUT's business.

Māori Data Sovereignty Māori data sovereignty concerns the rights and interests of Māori in relation to data that pertains to them, and ensures that data governance aligns with Māori values, aspirations, and philosophies. In the context of AUT and the Te Aronui framework, this translates to meaningful Māori involvement in decision-making processes around data management, safeguarding Māori intellectual property, and ensuring culturally sensitive data practices.

Software: the programs used to direct the operation of Hardware, including operating systems, patches and applications, and the documentation giving instructions on how to use that Software.

University: means the Auckland University of Technology (**AUT**) and includes all subsidiaries.

Users: all Users of AUT’s ICT systems including, but not limited to, all students, employees, contractors, consultants, other staff, suppliers and visitors.

4. SCOPE

This policy applies to all Users of AUT’s ICT systems including, but not limited to, all students, employees, contractors, consultants, other staff, suppliers and visitors.

All Users must comply with this policy and the associated procedures, guidelines and standards.

5. LEGISLATION AND COMPLIANCE

The University shall comply with all applicable New Zealand laws, legislation, and regulations.

See also the Register of Key Legislation and specifically:

General Academic Statute
Privacy Act 2020
Public Records Act 2005
Copyright Act 1994
Protected Disclosures (Protection of Whistleblowers) Act 2022
Unsolicited Electronic Messages Act 2007

8. RELATED PROCEDURES/DOCUMENTS

Information and Communication Technology Procedures
Discipline Policy
Intellectual Property Policy
Privacy Policy
Procurement Policy
Procurement Procedures
Records Management Policy
Records Management Procedures
Risk Management Policy
Risk Management Procedures
Social Media Policy
Te Aronui

10. DOCUMENT MANAGEMENT AND CONTROL

Policy Owner:	Chief Technology Officer
Last review:	15 September 2025
Next review:	30 September 2026
Approved by:	Vice-Chancellor
Effective date:	2 February 2024