ICT Acceptable Use Policy

Section 1 - Background

(1) This Policy governs the use of all Australian Catholic University (ACU) Information and Communication Technology (ICT) resources, including computers, software, networks, email systems, data storage, cloud services, telephone systems, and other digital communication facilities.

(2) This Policy applies to all members of the University community (including students, staff, contractors, vendors, and any individuals authorised to access ACU ICT resources), both on-campus and remotely, with ACU-owned or personal devices (BYOD).

(3) This Policy should be read in conjunction with other relevant ACU policies, including but not limited to:

a. Code of Conduct for Staff;
b. Misconduct and Serious Misconduct Policy;
c. Student Conduct Policy;
d. Discrimination and Harassment Policy;
e. ACU Staff Enterprise Agreement 2022-2025;
f. Privacy Policy;
g. Data and Information Governance Policy;
h. Research Data Management Policy;
i. Student Prevention and Response to Sexual Harm or Gender-Based Violence Procedure;
j. Staff Prevention and Response to Gender-Based Violence Procedure;
k. Workplace Bullying Policy and Procedure;
l. Employee Records Privacy Policy; and
m. Staff Sexual Misconduct Policy.

(4) Where there is any inconsistency between this Policy and another University policy dealing with staff or student conduct (including the Student Conduct Policy and Discrimination and Harassment Policy), the University may apply the policy or policies it considers most appropriate in the circumstances.

Section 2 - Purpose

(5) The purpose of this Policy is to:

a. Ensure ACU ICT resources are used responsibly, ethically, legally, and for purposes aligned with ACU's mission, values, and strategic objectives;
b. Protect the confidentiality, integrity, and availability of ACU's information assets and ICT resources;
c. Inform users of their responsibilities when accessing and using ACU ICT resources; and
d. Minimise risks associated with the misuse of ICT resources.

Section 3 - Principles

(6) Authorised Use: ACU ICT resources are provided primarily for teaching, learning, research, and administrative activities.

(7) Respect and Responsibility: Users are expected to use ICT resources in a manner that is lawful, ethical, respectful of others, and does not interfere with the work or study of others or the functioning of ACU ICT resources.

(8) Academic Freedom and Intellectual Property: ACU supports the use of ICT resources for academic inquiry and respects academic freedom and intellectual property rights. Users must comply with copyright laws and licensing agreements.

(9) Privacy: While ACU respects user privacy, users should be aware that data created, stored, or transmitted on ACU ICT resources may be subject to monitoring for security and compliance purposes (see Section 8).

Section 4 - User Responsibilities

Account Security

(10) Users are responsible for all activities conducted with an ACU account. Account access should be used solely for its intended purposes, and information access must be used in a responsible and ethical way.

(11) Passwords and authentication credentials must be kept confidential and must not be shared. Strong, unique passwords/passphrases must be used as per ACU guidelines. Multi-factor authentication (MFA) must be used where required. For latest advice, contact Service Central (for staff) or AskACU (for students).

(12) Users must lock computers or log out when unattended.

(13) Any suspected account compromise or security incident must be reported immediately to Service Central (for staff) or AskACU (for students).

Data Security and Management

(14) Users must:

a. Protect ACU data from unauthorised access, modification, disclosure, or destruction. Adhere to the ACU Data and Information Governance Policy and Research Data Management Policy;
b. Use only ACU-approved cloud storage and software-as-a-service (SaaS) platforms for storing or processing ACU information. For latest advice on this, contact Service Central (for staff) or AskACU (for students);
c. Ensure that external storage devices (e.g., USB drives) are not used to transfer sensitive ACU data without authorisation and security measures are in place; and
d. Ensure personal devices used to access ACU resources meet ACU's security requirements, including up-to-date antivirus software and security patches. Use all appropriate services provided by the university to enhance secure access to ACU resources.

Awareness

(15) Users are expected to take responsibility for developing an adequate level of information security awareness, education, and training to ensure appropriate use of the information environment.

Section 5 - Prohibited Users

(16) The following activities are prohibited when using ACU ICT resources:

a. Engaging in any illegal activity that violates local, state, or federal laws or regulations;
b. Unauthorised Access & Interference by:
    i. Attempting to bypass security measures or gain unauthorised access to any system, account, or data;
    ii. Disrupting or degrading network performance or the ability of others to use ACU ICT resources (e.g., network scanning, denial-of-service attacks); or
    iii. Sharing or using another person's account credentials.
c. Misuse of Resources by:
    i. Excessive or unauthorised use of network bandwidth or storage;
    ii. Sending spam, chain letters, or unsolicited bulk emails;
    iii. Using resources for unauthorised commercial activities, personal financial gain (unless part of approved ACU activities), or extensive political campaigning. Waging, betting, or excessive game playing that interferes with work or study;
    iv. Using Artificial Intelligence (AI) technologies unethically, for illegal activities, in ways that violate university policies, introduce bias, plagiarism, copyright infringement or create harmful applications; Use of Artificial Intelligence for teaching and research purposes must also comply with the Principles for Use of Artificial Intelligence in Teaching, Research and Operations;
    v. Using social media platforms and messaging apps for official ACU business not in compliance with ACU policies. Breaches of conduct via these channels, including inappropriate posting or sharing of confidential information, are subject to disciplinary action. Students and staff should exercise caution when posting on public or private platforms; or
    vi. Attempts to bypass security measures, introduce malicious software, install unauthorised software, or disrupt ACU ICT resources and external systems in any way.
d. Inappropriate Content & Conduct by:
    i. Creating, accessing, storing, displaying, or distributing offensive, pornographic, harassing, discriminatory, or threatening material, except in cases where such activities are conducted for legitimate, approved academic or research purposes with appropriate safeguards in place;
    ii. Harassment, bullying, intimidation, or defamation of others;
    iii. Violating copyright, patent, trademark, trade secret, or other intellectual property rights; or
    iv. Unauthorised sharing of Information: Disclosing confidential or proprietary ACU information without authorisation.
e. Conduct that may constitute discrimination, harassment, sexual misconduct, gender-based violence, vilification, bullying or other misconduct will be managed in accordance with the following policies
    i. Discrimination and Harassment Policy;
    ii. Misconduct and Serious Misconduct Policy;
    iii. Staff Prevention and Response to Gender-Based Violence Procedure;
    iv. Workplace Bullying Policy and Procedure;
    v. Staff Sexual Misconduct Policy;
    vi. Student Prevention and Response to Sexual Harm or Gender-Based Violence Procedure ;
    vii. Student Conduct Policy; or
    viii. Code of Conduct for Staff.

Section 6 - Personal Use of ICT Resources

(17) Minimal and incidental personal use of ACU ICT resources (e.g., personal emails, internet searches during breaks) is permitted provided it:

a. Occurs primarily during personal time (e.g., breaks, outside work/study hours);
b. Incurs no significant cost to ACU;
c. Is brief, infrequent, and does not interfere with official duties, academic responsibilities, or the work/study of others;
d. Does not compromise the security or integrity of ACU ICT resources or data; and
e. Complies with all other provisions of this Policy and relevant laws.

(18) Prohibited personal uses include conducting an outside business, extensive personal entertainment, or any activity listed in Section 5.

Section 7 - Personal Device Use (Bring Your Own Device (BYOD))

(19) Users connecting personal devices to ACU networks or accessing ACU resources via BYOD are responsible for:

a. Ensuring their device meets ACU's minimum security standards which include:
    i. an up-to-date anti-virus protection installed on the device;
    ii. PIN and/or passwords enabled upon start-up and/or login; and
    iii. and adhere to the Information Security Policy and Information Security Procedure.
b. Protecting any ACU data accessed or stored on the device. University digital information that is confidential or sensitive should not be stored on personal (BYOD) devices and all ACU information should be deleted promptly from the device once it is no longer needed;
c. Reporting loss or theft of a device containing ACU data immediately to their supervisor.

(20) ACU is not responsible for the maintenance, support, or loss/damage of personal devices.

Section 8 - Monitoring, Logging, and Privacy

(21) 21) ACU ICT resources and activities conducted on them may be monitored and logged by ACU for purposes including, but not limited to:

a. Ensuring the security, integrity, and performance of ACU ICT resources;
b. Investigating suspected policy violations or security incidents
c. Complying with legal and regulatory obligations; and
d. Managing resources and planning for future needs.

(22) This monitoring may include email, internet usage (sites visited, content, time spent), file access, and other electronic communications. Personal content stored on or generated using ACU ICT resources or ACU services may be subject to such monitoring, including:

a. Recording: Capturing and storing user activity data;

b. Auditing: Reviewing logs for threats and policy compliance;
c. Logging: Keeping detailed records of file and website access; and
d. Real-time inspections: Using software to monitor activities live, including automated decryption and inspection of data.

(23) While ACU respects user privacy, users should have no expectation of absolute privacy when using ACU ICT resources, except as protected by law. Monitoring, access and handling of personal information will be conducted in accordance with applicable Australian law, including the Privacy Act 1988 and Australian Privacy Principles, and the University's Privacy Policy and Employee Records Privacy Policy.

(24) The university may install monitoring software on ACU owned devices and services. Users must keep this software active and not disable or bypass it.

(25) ACU may restrict access to certain internet sites, services, or content and may limit email size or storage.

Section 9 - Outcome of Misuse

(26) Failure to comply with this Policy may result in disciplinary action, up to and including:

a. For students: Penalties as per the Student Conduct Policy, which may include exclusion or cancellation of enrolment;
b. For staff: Disciplinary action as per the Staff Enterprise Agreement and relevant policies and procedures, which may include termination of employment; or
c. For other users: Revocation of access privileges, termination of contracts, or other appropriate measures.

(27) Suspected illegal activities will be reported to law enforcement authorities.

(28) ACU may temporarily suspend access to ICT resources pending investigation of a potential breach.

Section 10 - Policy Review

(29) In accordance with the University's Policy Development Policy, this Policy is scheduled for review every 3 years.

(30) If any staff member wishes to make any comments about this Policy, they should forward their suggestions to the enquiries contact under the Status and Details tab.

Section 11 - Further Assistance

(31) Any staff member who requires assistance in understanding this Policy should first consult their nominated supervisor. Should further information or advice be required, staff should visit Service Central.

(32) Any student who requires assistance should contact AskACU.

Status and Details

Status	Current
Effective Date	8th May 2026
Review Date	8th May 2029
Approval Authority	Governance Officer
Approval Date	28th April 2026
Expiry Date	Not Applicable
Responsible Executive	Russell Parker Chief Information and Digital Officer
Responsible Manager	Peter Coppola Associate Director, Service Delivery
Enquiries Contact	Peter Coppola Associate Director, Service Delivery --- Information Technology