Acceptable Use of IT Resources Policy

Section 1 - Purpose

(1) This Policy outlines the standards of behaviour required for accessing the University's IT Resources.

Scope

(2) This Policy applies to all users of Macquarie University IT resources and connected systems. This includes:

a. staff employed by the University and its controlled entities;
b. students of the University including former students; and
c. affiliates including contractors, agents, honorary, clinical or adjunct appointees and consultants of the University.

Those listed above will be known as Users for the purpose of this Policy.

Background

(3) Macquarie University (the University) is committed to maintaining a secure technology environment and as such, has established behavioural requirements for accessing the University's IT Resources. Establishing these requirements aims to decrease the likelihood that IT Resources are misused.

Section 2 - Policy

(4) All Users should provide confirmation that they have read and understood this Policy prior to commencement of work/study at the University.

(5) Users provisioned with access to IT Resources should be aware of their responsibilities regarding appropriate care and protection.

(6) Unauthorised individuals must not be given physical or logical access to IT Resources or Information.

(7) The owner of a User account is solely responsible for all actions performed using their account.

(8) IT Resources may be used for acceptable limited and reasonable personal use. Such personal use must be lawful, not negatively impact the University or violate this Policy. See the Acceptable Use of IT Resources - Misuse Schedule for examples of unacceptable use.

(9) Users should consider the implications of storing and transmitting personal information not required by the University within IT Resources (e.g., personal events, security clearances, passports, files containing personal information, etc). The University is not responsible for protecting such Information.

(10) Fixed IT Resources (e.g., monitors, routers) must not be taken off-site without prior written authorisation by the IT Service Desk or an authorised manager.

(11) Information created, sent, received, or processed for the University's business purposes that is not subject to the

intellectual property rights of Users, is owned by the University.

Incident Notification

(12) Users have a responsibility to maintain vigilance and report any suspicious cyber security events occurring against the University, in accordance with this Policy and the Data Breach Policy. This includes:

a. IT Resources behaving differently or unusually;
b. University emails which are suspected to be malicious or suspicious;
c. individuals asking for user credential (e.g., username and password);
d. loss/theft, or suspicion of loss/theft of IT Resources; and
e. breaches of this Policy or other cyber security policies.

(13) University related cyber security events should be reported immediately to the IT Service Desk team or the IT Cyber Security team (cyber@mq.edu.au). Details of cyber security events should remain confidential and not be divulged or discussed with unauthorised individuals.

(14) The University is not responsible for managing cyber security breaches for the personal emails, accounts or devices of Users. However, Users are encouraged to report incidents where there is a potential impact to University IT Resources.

Protection of Physical IT Resources

(15) IT Resources must:

a. not be left unlocked while unattended;
b. not be connected to public Wi-Fi;
c. not be left unattended in public areas or in motor vehicles;
d. be up to date with the latest software patches installed (e.g., browsers and operating systems);
e. have Wi-Fi and Bluetooth auto-connecting capabilities disabled if not in use; and
f. have wireless file sharing capabilities disabled (e.g. 'AirDrop' on iOS or 'Nearby Share' on Android).

(16) Untrusted removable storage media (e.g., USB drives and external hard drives) should not be connected to IT Resources.

(17) IT Resources should only be charged using trusted charging devices (e.g., charger, cables, power adapter). Public charging stations or USB ports (e.g. airports, restaurants, conference rooms) should not be used.

(18) On the last day of employment or termination of a contract, staff and affiliates must return all University IT Resources and any associated accessories (e.g., keyboards, chargers, travel cases).

(19) Students must return IT Resources when they are no longer required for study purposes.

Protection of Information

(20) Information should be generated, stored, processed and transmitted in accordance with the:

a. Information Classification and Handling Procedure;
b. Records and Information Management Policy; and
c. Privacy Policy.

(21) Personal email or cloud storage accounts should not be used to store, process or transmit University owned

Information.

(22) Information classified as Confidential or above (refer to the Information Classification and Handling Procedure) should be securely stored when not in use or when left unattended.

(23) Information that is no longer required should be securely disposed of in accordance with the Records and Information Management Policy and approved retention schedules, using appropriate disposal methods for the information type, including secure digital deletion, system-based disposal, or media sanitation.

(24) Whiteboards and other Information display sources should be cleaned of any Information classified Confidential or above, after use.

Remote Working and Travel

(25) Home Wi-Fi should be password protected with the latest supported Wi-Fi security protocols, if used to connect to University IT Resources.

(26) Staff must comply with travel requirements detailed in the Travel Policy.

Cyber Security Training

(27) Staff must complete cyber security awareness training as required by the University.

Monitoring and Privacy

(28) The University monitors all its IT Resources in accordance with the University's Workplace Surveillance Policy. Breaches of this Policy constitute misuse of the University's IT Resources.

(29) The University may access, review, monitor, or disclose the contents of all messages created, sent or received using IT Resources. This may be performed for monitoring compliance with this Policy, terms and conditions of employment/engagement, and statutory obligations.

(30) Users should assume that personal information transmitted by or stored on University IT Resources will be accessed by the University to the extent permitted by law. Any personal information managed by the University will be handled in accordance with the Privacy Policy and the Workplace Surveillance Policy.

(31) The University may refer serious matters or repeated breaches to the Chief Information and Digital Officer, Chief People Officer, the Head of the relevant organisational unit, or the appropriate external authorities, which may result in disciplinary, civil and/or criminal proceedings.

(32) The University has a statutory obligation to report unlawful activities, serious wrongdoing and corrupt conduct to appropriate authorities and will cooperate fully with the relevant authorities.

Prohibited Conduct

(33) Users must not use IT Resources for, or in support of, illegal, obscene, or other inappropriate activities, in accordance with the Acceptable Use of IT Resources - Misuse Schedule.

Compliance and Exemptions

(34) Any exemption to this Policy must be sought from the Chief Information Security Officer (CISO).

(35) Breaches of this Policy by staff and students will be managed in accordance with the applicable provisions of the Student Code of Conduct, Student Conduct Rule, Student Conduct Procedure, Staff Code of Conduct and other relevant policy instruments.

Section 3 - Procedures

Use of Personal Mobile Devices

(36) The University permits staff to access University Information and applications via their personal mobile devices.

(37) To maintain the security of University Information, personal mobile devices used to access University Information and applications must:

a. be configured to automatically lock and require authentication (e.g., facial recognition, fingerprint scan, or a pin code to unlock);
b. be actively supported by the device vendor;
c. be capable of running the University approved Multi-Factor Authentication (MFA) application;
d. be kept up to date with the latest operating system/security updates;
e. have missing or stolen devices that had access to work applications reported;
f. not access sensitive corporate data in areas where there is oversight;
g. not be jailbroken or non-baseline built in anyway; and
h. not access corporate information when overseas without an active exemption in place (see the Travel Policy).

(38) If the above cannot be met personal mobile devices must not be used and either use of corporate laptop or corporate device is required in place.

(39) The University is not responsible for any loss of personal data, delays, non-deliveries, service interruptions, technical difficulties, or malicious activity to a personal mobile device.

Internet, Email, Social Media and Artificial Intelligence (AI) Usage

(40) The University permits staff to access internet, email, social media and Artificial Intelligence (AI) for the following reasons:

a. to carry out their duties and contribute to the University's goals and objectives;
b. for initiating and furthering professional contacts;
c. for personal development; and/or
d. where authorised, for communicating to wider stakeholder and community groups.

(41) Staff should:

a. take all reasonable care when downloading, accessing or executing files from the internet;
b. carefully consider the type and nature of Information requested when browsing the internet;
c. be aware of copyright restrictions; and
d. ensure that non-work-related email addresses are not included in work related correspondence;

(42) University approved AI tools should be used in accordance with the Responsible and Ethical Use of Artificial Intelligence Policy.

(43) University data must not be uploaded to non-university managed AI tools.

(44) Social media should be used in accordance with the Social Media Policy.

Section 4 - Guidelines

(45) Nil.

Section 5 - Definitions

(46) The following definitions apply for the purpose of this Policy:

a. AI (Artificial Intelligence) has the meaning provided in the NSW AI Assurance Framework, being “intelligent technology, programs, and the use of advanced computing algorithms that can augment decision-making by identifying meaningful patterns in data”.
b. Information means any information in either physical or electronic format that is generated, created, stored, purchased or received during the conduct of University operations.
c. Information Technology Resources, or IT Resources, includes, but is not limited to:
    i. All computers and all associated data networks and systems, internet access and network bandwidth, email, hardware, data storage, computer accounts, all OneID systems, media, software (both proprietary and those developed by the University) and telephony services.
    ii. Information Technology services provided jointly, or as part of a joint venture between the University and a research centre, school, institute affiliated with the University, a subsidiary organisation owned by the University or any other partner organisation.
    iii. Information Technology services provided by third-parties that have been engaged by the University.

Status and Details

Status	Current
Effective Date	23rd July 2026
Review Date	23rd July 2031
Approval Authority	Deputy Vice-Chancellor (People and Operations)
Approval Date	23rd July 2026
Expiry Date	Not Applicable
Responsible Executive	Eric Knight Deputy Vice-Chancellor (People and Operations)
Responsible Officer	Jonathan Covell Chief Information and Digital Officer
Enquiries Contact	Andrew Karvinen Chief Information Security Officer