Information Technology Procedure - Acceptable Use and Access

Section 1 - Purpose

(1) This procedure supports the Information Technology Policy and sets out detailed information and requirements to:

a. facilitate the efficient, effective, responsible and lawful use of the University's information and communication (ICT) resources
b. safeguard the interests of the University and all authorised users of its ICT resources
c. provide guidelines and instructions to authorised users in the appropriate use of the University's ICT resources.

Scope

(2) This procedure applies to all authorised users, ICT resources and controlled entities as defined in the Information Technology Policy.

Section 2 - Policy

(3) See the Information Technology Policy.

Section 3 - Procedure

Part A - Providing access to ICT resources

(4) The University provides secure access to ICT services and resources for all students, staff and other authorised users, for the purpose of pursuing and advancing its object and functions.

(5) Secure access to electronic information and communication services is available to University staff during periods of authorised access from University managed locations and managed devices.

(6) Secure access to electronic information and systems implemented to provide and progress a student's study and interactions with the University is available continuously to students during periods of authorised access from University managed locations.

(7) Additional access via remote access platforms is provided for staff and students, and is delivered via highly available infrastructure that limits unplanned outages to those required for essential maintenance only.

(8) University ICT resources:

a. are reviewed and monitored to ensure proper functioning
b. remain the property of the University at all times.

(9) The University reserves the right to recover or otherwise protect University ICT resources, including University

hardware, communications devices, storage media, data, information, and records.

(10) The University accepts no responsibility for any damage to or loss of data arising directly or indirectly from use of ICT resources or for any consequential loss or damage.

(11) Authorised users will be provided with a unique username and password to enable access to University ICT systems and facilities. These will be provided:

a. for employees, once the acceptance of employment offer and/or other appointment documentation has been received by the University and entered into the Division of People and Culture's human resource management system
b. for new students, at the point of accepting their offer
c. for visitors (temporary staff, contractors, consultants, etc), when a temporary access account is created.

(12) Authorised users will be provided with other information and guidance to ensure they are aware of the conduct expected of them when using University ICT resources in alignment with relevant industry standards.

(13) An authorised user's access will be removed after their enrolment, employment or engagement with the University has ended.

Part B - Acceptable use

Obligations

(14) Authorised users must:

a. only use University ICT resources for activities related to the functions and objects of the University, or as otherwise allowed by this procedure
b. take every reasonable precaution to secure their University login identification across all devices (including personal devices)
c. comply with state and Commonwealth legislation, University policies and other directives that may be issued by the University regarding the use of ICT resources from time to time
d. only use AI tools in ways that adhere to the S.E.C.U.R.E. GenAI Use Framework for Staff, Statements of Principles of the use of Artificial Intelligence, and the AI Risk Management Framework (AI RMF). Use of AI tools must align with the governance, risk mitigation and ethical standards outlined in these frameworks.
e. take reasonable care to prevent damage, loss, theft, or unauthorised access and use of University ICT resources
f. co-operate and participate in the appropriate use of University ICT resources
g. complete the mandatory training within the first month of employment and annual recertification when required (supervisors and managers are responsible for providing all other IT induction and training required by employees in their organisational units)
h. report ICT incidents to SX Service Centre (students) or the IT Service Desk (all other authorised users) including:
    i. damaged, lost or stolen University ICT resources
    ii. suspected or known data security breaches
    iii. any threats, intimidation or harassment received through University ICT resources
    iv. any other known breaches of this procedure (see also the Compliance Management Procedure regarding identifying and reporting compliance breaches).

Prohibited use

(15) Subject to clause 16, authorised users must not:

a. obtain or attempt to obtain a higher than authorised level of privilege on any University ICT resource
b. abuse, remove or tamper with any University ICT resources
c. introduce viruses or any other software or technology designed to disrupt, corrupt or destroy University programs and/or data
d. introduce or use unapproved software
e. attempt to breach University system security
f. dispose of or remove from the University's control any University ICT resources, including University data, information or records, without appropriate approval
g. access, examine, copy, rename, change, disclose or delete programs, files, messages, data, information, records or hardware belonging to the University or any other authorised users
h. access, alter, disclose or expose personal or health information held by the University without appropriate authorisation
i. alter any restrictions associated with any University computer system, computer account, network system, personal computer software protection or any other University ICT resources
j. remove, deface or corrupt notices placed by University staff regarding the use of University ICT resources
k. disclose their University password or other authentication credentials to any other parties, or otherwise allow other parties access to any ICT resources via their authentication credentials
l. use or attempt to discover the password or other authentication credentials of another user
m. use the University's ICT resources for any non-University business activities or personal gain, subject to the personal use provisions of this procedure
n. use University ICT resources to engage in illegal activities, including but not limited to making, sending or storing fraudulent, unlawful, harassing or abusive calls or messages
o. impede the efficient and effective operation of University ICT resources (e.g. unauthorised bulk, spam, phishing or all user e-mails)
p. access, transfer, publish, display, circulate or store prohibited material, messages or data that contravenes University rules, policies, procedures and/or guidelines
q. store University data in an unauthorised storage area, service or location, including cloud storage, USB, or other personal storage devices
r. illegally store, transfer or reproduce copyrighted material or otherwise infringe another party's intellectual property, copyright or moral rights
s. configure email rules that automatically forward received emails to external recipients.

(16) Subject to appropriate delegated approval, the provisions of clause 15 may be waived where an authorised user is required to carry out any of these acts in the performance of duties directly related to their work or, in the case of students, to their academic program.

Personal use of ICT resources

(17) The University will allow employees reasonable personal use of ICT resources, with the exception of activities prohibited under clause 15, where such use has no negative impact on the employee in the performance of their duties or adverse impact on the University ICT resources. Noting that staff must not use personal email or cloud services to store, transmit, or share University data. This activity is strictly prohibited under Clause 15(f). The University is reviewing technical controls to mitigate this risk. Until such controls are implemented, this clause will be monitored for compliance and may be subject to further restriction.

(18) Current students may use University ICT resources for personal use, with the exception of activities prohibited under clause 15, in accordance with this procedure.

Breach of acceptable use

(19) The University will monitor and audit the use of ICT resources.

(20) As per the Surveillance Procedure, the University will not prevent or block emails or internet access of any authorised user except as permitted under the Workplace Surveillance Act s 17, this procedure, or other University policy. The University is not obliged to notify a worker that it has prevented delivery of an email if:

a. the email was a commercial electronic message, within the meaning of the Spam Act 2003 (Cth)
b. the content or attachments of the email would or might result in unauthorised interference with, damage to or operations of a network or ICT resource (including any program run or data stored on any ICT resource)
c. the University regards the content of the email, including any attachment(s), as menacing, harassing or offensive
d. the sender of the email has been identified as having previously sent malicious content to the organisation
e. the University is not aware (and cannot reasonably be expected to be aware) of whether a worker has sent that email or of the identity of the employee who has sent that email.

(21) All authorised users must report breaches of this procedure.

(22) The Chief Operating Officer may authorise an investigation where there are reasonable grounds to suspect that a breach of this procedure has occurred, on the recommendation of relevant University officers (including but not limited to the Chief Information and Digital Officer (or nominee), Director, Security and Resilience (CSO), General Counsel, the University's public interest disclosure officer (under the Public Interest Disclosure (Whistleblowing) Policy) and/or the University's privacy officer (under the Privacy Management Plan).

(23) Subject to the authorities to access information under Delegation Schedule A - Governance and Legal, an investigation may include (but not be limited to):

a. email use
b. internet use
c. storage of data on ICT resources
d. storage of data
e. telephone and mobile device usage.

(24) Authorised user accounts and access to ICT resources (in full or in part) may be suspended while a potential, suspected or actual breach of the ICT Policy or related procedures is investigated (as per Delegation Schedule D - Facilities and Information Technology).

(25) Misuse of University ICT resources and/or failure to comply with the ICT policy or related procedures may result in:

a. for students, the action being reported as general misconduct for action under the Student Misconduct Rule 2020
b. for staff, the action being deemed a breach of the Code of Conduct and subject to any sanctions under that
c. for other authorised users, suspension or termination of their access to University ICT resources and other actions in accordance with any contracts or agreed terms of use
d. legal or criminal proceedings.

(26) Notwithstanding clause 25, the University will report illegal activity to police or any other appropriate authority external to the University.

Part C - ICT support and training

(27) The Division of Information Technology will provide the following core information technology services at the desktop of University employees:

a. IT Service Desk for help and support
b. training modules
c. access to the internet
d. online access to the University's academic and administrative information and services
e. standard suite of category one software, including MS Office and web browser.

(28) Requests for non-core services must be submitted to the division by an organisational unit manager and approved by the Chief Information and Digital Officer.

Section 4 - Guidelines

(29) Nil.

Section 5 - Glossary

(30) For the purpose of this procedure:

a. Authorised User - includes, but is not limited to:
    i. staff
    ii. adjuncts
    iii. students - persons enrolled in a course or subject
    iv. persons who are affiliated or associated with the University who are granted a temporary access account and provided with authentication credentials. Examples include:
        - research associates
        - community groups
        - vendors and contractors
        - board members
        - visiting fellows
    v. eduroam users from other educational institutions.
b. Bring your own device (BYOD) - non-University equipment (such as laptops, smartphones, tablets and similar devices) that connect to the University's network.
c. Confidential and sensitive material – as defined in the Information Classification and Handling Procedure.
d. Phishing – attempting to acquire information such as usernames, passwords and credit card details by sending an email that appears to be from a legitimate business, organisation or individual.
e. Prohibited material – as defined within relevant Commonwealth and State legislation including, but not limited to:
    i. descriptions or depictions, expressly or otherwise of matters of sex, drug misuse or addiction, crime, cruelty, gambling, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of decency and propriety generally accepted by reasonable adults

ii. describes or depicts a minor who is, or who appears to be, under 16 years of age, whether the minor is engaged in sexual activity or not, in a way that is likely to cause offence to a reasonable adult, promotes, incites or instructs in matters of crime or violence

iii. discriminates against, harasses or vilifies any member of the public on the grounds of sex characteristics, gender identity, pregnancy, age, race, nationality, descent or ethnic background, religious background, marital status, disability, medical conditions, sexual orientation

iv. defames or could be reasonably anticipated to defame, any person, institution or company.

f. Personal information - as defined in the Privacy Management Plan.

Status and Details

Status	Current
Effective Date	10th December 2025
Review Date	10th December 2030
Approval Authority	Chief Operating Officer
Approval Date	10th December 2025
Expiry Date	Not Applicable
Unit Head	Helen Jessop Chief Information and Digital Officer
Author	Hannah Madden Executive Officer
Enquiries Contact	Division of Information Technology