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 and ICT resources, 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 continuously 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 must acknowledge this procedure and will be provided with other information and guidance to ensure they are aware of the conduct expected of them when using University ICT resources (as required by ISO 27002 section 5.1 - Information security, cybersecurity and privacy protection — Information security controls).

(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. take reasonable care to prevent damage, loss, theft, or unauthorised access and use of University ICT resources
e. co-operate and participate in the risk assessment and management of University ICT resources
f. report the following incidents to Student Central (students) or the IT Service Desk (all other authorised users):
    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 Assurance 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
r. illegally store, transfer or reproduce copyrighted material or otherwise infringe another party's intellectual property, copyright or moral rights.

(16) The provisions of clause 15 do not apply 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.

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

(21) 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 Executive Director, Division of Information Technology (or nominee), Chief Security Officer, General Counsel, the University's public interest disclosure officer (under the Whistleblowing (Reporting Wrongdoing) Policy) and/or the University's privacy officer (under the Privacy Management Plan).

(22) 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 on shared network services
e. telephone and mobile device usage.

(23) Authorised user accounts and access to ICT resources (in full or in part) may be suspended for up to 14 days 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).

(24) 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.

(25) Notwithstanding clause 24, the University will report illegal activity to police or any other appropriate authority external to the University.

Part C - ICT support and training

IT induction and training for employees

(26) The following online IT induction training modules assist University employees in using University IT facilities. Mandatory modules must be completed within the first month of employment and annual recertification may be required.

a. IT Fundamentals - ELMO Module (recommended for all staff)
b. Information Security Awareness - ELMO Module (mandatory for continuing and fixed-term staff)
c. Information Security Awareness for Casual Staff - ELMO Module (mandatory for casual staff and visitors)
d. Classroom Technology at CSU - ELMO Module (recommended for academic staff)

(27) Supervisors and managers are responsible for providing all other IT induction and training required by employees in their organisational units.

Desktop support services

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

a. access to the internet
b. online access to the University's academic and administrative information and services
c. the ability to effectively operate the standard suite of category one software, including MS Office and web browser

d. the ability to print to a networked printer within the near vicinity.

(29) Requests for non-core services must be submitted to the division by an organisational unit manager and approved by the Executive Director, Division of Information Technology, including:

a. the installation of hardware upgrades and peripherals (including printers) onto individual workstations
b. the installation of category two or three software (i.e. products that are not part of the standard suite of University applications) onto individual workstations
c. the installation of additional network printers within a particular unit
d. supporting networked printers as opposed to printers installed on individual workstations
e. entering into an agreement with an external supplier to repair standard items of AV equipment, including such things as overhead projectors, video recorders, data projectors and television monitors
f. allowing sectional managers to have approved non-core software installations, hardware upgrades and peripheral installations carried out by authorised external contractors on a fee for service basis.

Section 4 - Guidelines

(30) Nil.

Section 5 - Glossary

(31) For the purpose of this procedure:

a. Authorised User - includes:
    i. staff
    ii. students - persons enrolled in a course or subject
    iii. 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
    iv. 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 - any information or material including but not limited to:
    i. staff or student personal information
    ii. unpublicised strategic, legal, financial or research information, and
    iii. any data that could compromise any facet of the University, including reputation.
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, pregnancy, age, race, nationality, descent or ethnic background, religious background, marital status, disability, medical conditions, sexual preference, homosexuality and transgender

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	1st August 2022
Review Date	1st August 2025
Approval Authority	Chief Operating Officer
Approval Date	30th July 2022
Expiry Date	Not Applicable
Unit Head	Mark Duffy Executive Director, Division of Information Technology
Author	Vanessa Salway Manager, Policy and Records
Enquiries Contact	Division of Information Technology +61 2 63386260