IT Acceptable Use Policy

Section 1 - Purpose of Policy

(1) The University is committed to the appropriate use of information technology and services to support its learning, teaching, research, administrative, and service functions. This Policy defines acceptable behaviour expected of users of University IT facilities and services. The University requires users to comply with the IT policy documents and associated requirements governing the use of IT facilities and services as a condition of their use. These are accessible on the University Policy Directory.

Section 2 - Application and Scope

(2) This Policy applies to all use of University IT facilities and services. It covers computing, collaboration and communications facilities, examples of which include telephones, facsimiles, mobile telephones, computers, tablets, printers, photocopiers, other devices, email, internet access, network infrastrucure, web services, cloud services and similar resources.

(3) Use of remote systems accessed via IT facilities and services is also covered by this Policy. Remote services may have additional local rules and regulations.

(4) Users must accept and comply with University IT policies as a condition of use. This Policy is designed to allow legitimate, secure and optimal use of IT facilities and services.

Section 3 - Policy Principles

(5) IT facilities and services are provided to users to conduct teaching, learning, research and administrative pursuits.

(6) Users must take responsibility for using IT facilities and services in an ethical, respectful, secure and legal manner; having regard for the objectives of the University and the privacy, rights and sensitivities of other people.

Section 4 - Authorised Use, Access and Authentication

(7) Users are authorised to use University IT facilities and services when assigned a user account subject to the conditions in this Policy. Authority to use IT facilities and services is not normally granted by other means. This does not apply to public services, which do not require authentication to access. All staff and students must have a user account to be able to use IT facilities and services.

(8) User account creation and management is governed by the IT User Account Management Procedures.

(9) IT facilities and services require authentication in order to access, and most require multi factor authentication (MFA). Access is further controlled based on roles, which are linked with the username of a user account.

(10) Some IT facilities and services are provided for specific functions only and may only be used by specifically authorised users.

(11) Users must use IT facilities and services only in the manner intended for their role.

(12) Users must not share their user account, password or other authentication credentials. users must not use an account assigned to somebody else. This does not apply where authorised IT support staff are conducting their duties and the user has provided their credentials in the course of receiving support.

(13) Users must set up the self-service password reset capability to enable themselves to reset a forgotten or expired password.

(14) Users are discouraged from recording passwords on paper. A secure password management system is recommended if needed.

Security

(15) Users have a responsibility to be vigilant and know how to protect themselves and IT facilities and services. Cyber Security Awareness Training is mandatory for all staff.

(16) For new staff, Cyber Security Awareness Training is mandatory as part of their onboarding and probation requirements.

(17) Managed computers that are compromised will be reset to the standard image and software reinstalled by IMTS support staff.

(18) All software on devices must be kept up to date to ensure known security vulnerabilities are fixed.

(19) All devices must have security features such as password protection, firewall and anti-virus/anti-malware enabled where available.

(20) Attackers use the web to target users. users must take care when browsing webpages. The following actions help protect against web attacks:

a. browsers and all plugins must be kept up to date with security fixes;
b. unnecessary browser plugins should be avoided;
c. before authenticating to online applications or content or entering private data, ensure the connection is secure and thesite is secure; and
d. software must not be installed if prompted. Software should only be installed if the User is authorised to do so and has deliberately downloaded the software from a trustworthy source.

(21) The University uses various network and device security controls to help protect from cyber-attacks. Occasionally, these controls may interfere with user experience, users must not subvert nor attempt to subvert any security control.

(22) Access to a user account may be temporarily suspended if the account is suspected to be compromised and is posing an unacceptable risk.

(23) users must not give means to a third-party to access IT facilities and services without approval from IMTS.

(24) The University may conduct threat simulations designed to enable the University to assess vulnerabilities and raise awareness regarding common attacks and how to deal with them. This may include phishing simulations, where a user’s email address details are used to send simulated phishing emails. Phishing emails are malicious emails designed to entice users to visit fake and forged online content to steal usernames and passwords or download

malware or viruses. In such simulations, the University will not use any such information that may be entered by users but will use aggregated information generated from such simulations to help protect both user and University security through enhanced controls and awareness.

Conduct and Activity

(25) Users are responsible for the following whilst using the IT facilities and services:

a. all activities that originate from their user account;
b. all information sent from, intentionally requested, solicited, or viewed from their user account; and
c. information placed on a device using their user account.

(26) Users must not use the IT facilities and services for the following activities:

a. the creation or transmission (other than for properly supervised and lawful teaching or research) of any material or data that could reasonably be deemed abusive, offensive, defamatory, obscene or indecent;
b. the creation or transmission of material that could reasonably be deemed likely to harass, intimidate, harm or distress;
c. the unauthorised transmission of material that is labelled confidential or commercial in confidence; or
a. deliberate unauthorised access to IT facilities or services

Using devices and Equipment

(27) Users will be held responsible for cost of repair if damage is caused to IT equipment through misuse or negligence. Damaged equipment that may cause harm must not be used. Damage to IT equipment must be reported to IT support staff.

(28) IT facilities and services must not be tampered with or moved without authorisation.

(29) When using computer laboratories, rules, signs, and instructions from IT support staff must be complied with. Users must provide identification to support staff if requested.

(30) Users must return all devices if no longer employed by the University, the assets are no longer needed or if directed by the relevant Senior Executive, Executive Dean or Director.

Personally Owned devices

(31) Users may use a personally owned device to access IT facilities and services on the following terms:

a. users may connect to the University Wi-Fi network or remotely access services via Internet;
b. users must not connect a personally owned device to a wired network port without authorisation;
c. users must comply with this Policy;
d. users must maintain good security hygiene of the personally owned device, including the following:
    i. ensure all software and personally owned devices have the latest updates applied;
    ii. use security software and configure security features such as firewall and anti-virus / anti-malware; and
    iii. password protect their personally owned device.
        - a personally owned device must not be used where it is known to have a security compromise. users must reinstall the operating system and all software from trustworthy sources before continuing to use the personally owned device.
        - users must not store any non-public University data on a personally owned device.

Cloud Computing & External IT Services

(32) Procurement of externally hosted IT services must comply with the Purchasing and Procurement Policy.

(33) Users must not store or backup non-public University data with externally hosted services other than where provided through and approved by IMTS.

Student Use of Software

(34) Users may use a personally owned device to access IT facilities and services on the following terms:

a. users may connect to the University Wi-Fi network or remotely access services via Internet;
b. users must not connect a personally owned device to a wired network port without authorisation;
c. users must comply with this Policy;
d. users must maintain good security hygiene of the personally owned device, including the following:
    i. ensure all software and personally owned devices have the latest updates applied;
    ii. use security software and configure security features such as firewall and anti-virus / anti-malware; and
    iii. password protect their personally owned device.
e. a personally owned device must not be used where it is known to have a security compromise. users must reinstall the operating system and all software from trustworthy sources before continuing to use the personally owned device.
f. users must not store any non-public University data on a personally owned device.

(35) Exemptions by request directly to IMTS may apply to PhD research students using IT facilities and services provided to carry out their research. Any software that is to be installed on these facilities must comply with the Purchasing and Procurement Policy.

Non-University Use of IT facilities and services

(36) IT facilities and services are provided to support the University's teaching, research, administrative and services purposes.

(37) The University accepts that users will on occasion use IT facilities and services for incidental personal purposes. users must balance use for personal purposes with the management of resources in an efficient, economical, and ethical manner. They must ensure use does not:

a. interfere with the operation of IT facilities and services;
b. interfere with other users access to IT facilities and services;
c. burden the University with additional costs; or
d. interfere with their employment or other obligations to the University.

(38) users are not permitted to use the IT facilities and services for:

a. unauthorised commercial activities;
b. unauthorised personal gain; or
c. unauthorised gain to a third-party.

Email and Internet Services

(39) IT facilities and services are provided to support the University's teaching, research, administrative and services purposes.

(40) The University accepts that users will on occasion use IT facilities and services for incidental personal purposes. Users must balance use for personal purposes with the management of resources in an efficient, economical, and ethical manner. They must ensure use does not:

a. interfere with the operation of IT facilities and services;
b. interfere with other users access to IT facilities and services;
c. burden the University with additional costs; or
d. interfere with their employment or other obligations to the University.

(41) Users are not permitted to use the IT facilities and services for:

a. unauthorised commercial activities;
b. unauthorised personal gain; or
c. unauthorised gain to a third-party.

Telephones and Mobile devices

(42) The use of telephones and mobile devices must comply with this Policy and the Telephone and Mobile Use Policy

(43) the Acceptable Expense Guidelines outline responsibilities for costs incurred regarding home internet and telecommunications.

Data Governance

(44) Each University data element, as defined in and limited by the scope of the Data Governance Procedure, must have a custodian accountable for, including but not limited to, data access, definition, quality and privacy compliance.

(45) The types and duties of custodians responsible for the governance of University data are set out in the Data Governance Procedure.

Data Access, Classification and Quality

(46) Users are responsible for appropriately handling University data and must comply with relevant University Policies such as the Privacy Policy, IP Intellectual Property Policy, Records Management Policy, Research Data Management Policy, Travelling Overseas with Devices Procedure, Data Handling Guidelines, and Data Governance Procedure.

(47) Collection, access authorisation, and use of data must be underpinned by a relevant business need.

(48) Responsibilities for providing access to data are outlined in the Data Governance Procedure and Delegations of Authority Policy.

(49) Technical controls (e.g. file permissions and authentication) must be used to restrict access to authorised users only.

(50) University data assets, as defined in the Data Governance Procedure, must be assigned a level of security classification to ensure appropriate handling and protection.

(51) The Data Handling Guidelines provide best practice guidance on how to protect and handle data based on security classification of its data assets.

(52) Users must consider security requirements of any University data they handle. All University data must be handled to avoid unintended disclosure or loss.

Data Storage

(53) Only data storage solutions provided by IMTS, including approved cloud solutions, are suitable for storing University data. These solutions are accessed via the network, have authentication, and access controls, and provide a high level of protection from data loss by maintaining copies in multiple sites and use highly redundant technology.

(54) University data must be stored to avoid accidental loss. It is not sufficient to rely on storage devices in desktops, laptops, external/portable drives, tablets, and telephones.

(55) All University data must be primarily stored (or have a current copy stored) on enterprise storage provided through IMTS.

(56) University data must not be stored on external portable storage, personally owned devices, personal cloud storage or personal email accounts.

(57) Data defined as highly restricted in the Data Governance Procedure must not be stored on University devices and should be stored on University managed file servers (such as H: or S: drives) or approved cloud solutions.

(58) It is common for user devices to fail and cause loss of all data stored on the device. Be aware that the hard drive, desktop and 'my documents' folders are not automatically backed up. users must maintain current copies of data on enterprise storage systems.

(59) Devices which are no longer required, and which contain University data, must be disposed of securely to avoid accidental disclosure. users should consult with IMTS for advice before proceeding with such activity.

Copyrighted Software and Content

(60) Users are responsible for making use of software and electronic materials in accordance with the Copyright Act 1968 (Commonwealth), software licensing agreements, and any applicable University policies including the Copyright Policy.

(61) Unauthorised copying or communication of copyright protected material (including music and videos) violates the law and is contrary to the University's standards of conduct and business practices. The University may enforce controls within the institution to prevent the copying or use of unauthorised music, videos, and software.

Dealings in Copyright Protected Material for Teaching or Research

(62) Staff and students can copy and or communicate copyright protected material for teaching or study purposes where they have the permission of the copyright owner. Limited permission may be granted, for example, via website statements, license agreements, or under the statutory license provisions of the Copyright Act 1968 (Commonwealth).

(63) Staff and students may also be able to copy limited portions of material under the 'fair dealing' provisions of the Copyright Act 1968 (Commonwealth).

(64) For more information on what, and how much, users can copy and communicate under the fair dealing and statutory license provisions of the Copyright Act 1968 (Commonwealth).

Section 5 - Privacy

(65) The University is committed to complying with privacy requirements and confidentiality in the provision operation of all IT facilities and services. Users must comply with the Privacy Policy whilst using IT facilities and services. For further information refer to the Privacy webpage.

(66) User's names and usernames will be listed in directories accessible to other users for the purpose of enabling collaboration.

(67) Users must be aware that unless encrypted, stored data and data in transit via the network may be able to be accessed by unauthorised persons. users should use secure network protocols for transferring data on the internet.

(68) When using a multi-user system, users must be aware that many of the activities undertaken may be visible to other users.

(69) Logs of User activity are maintained by IMTS for troubleshooting, accounting, security investigations, reporting and legal purposes. These logs include times of sent and received email; email addresses (both sender and recipient), network activity metadata, web sites visited, telephone call records, and computers and services accessed. These logs are stored securely and are retained for legal requirements.

(70) Authorised IT staff may incidentally observe data during the course of their duties.

(71) In the case of an emergency or crisis, personal data, such as email addresses or phone numbers may be used to notify a User of the incident.

Computer Surveillance

(72) The University will conduct ongoing and intermittent computer surveillance of all users and devices/personally owned devices which access the IT facilities and services for the purpose of:

a. protecting its assets, property and finance from suspected unlawful activities or activities which are in breach of University Policy or Rules;
b. conducting its business and operational requirements;
c. protecting its reputation;
d. compliance with legislative requirements; and
e. meeting the expectations of stakeholder and the general public.

(73) The University is committed to meeting its statutory obligations under the Workplace Surveillance Act 2005 (NSW) and this Policy represents formal notification to users about activities of the University that fall within the definition of computer surveillance.

(74) Computer surveillance will be carried out by all means available to the University including but not limited to:

a. accessing University email accounts or emails;
b. accessing files;
c. accessing work devices, including activity logs;
d. recording internet usage and accessing these records;
e. accessing telephone usage logs; and
f. accessing personal devices that have been used to conduct University business.

(75) Users acknowledge that Computer Surveillance may include logging and monitoring of a User's access and use of wireless and telecommunications systems that form part of the IT facilities and services, including using devices or personal devices. This may include information which enables identification of the User's or device's location when accessing the University's systems, for example, when a User accesses a wireless access point in a specific location on the University's premises.

(76) Users acknowledge that Computer Surveillance may result in the prevention of:

a. delivery of an email sent to or by a user;
b. access to an internet website and other online content; or
c. access to software applications.

(77) The University will notify the User as soon as practicable that an email has not been delivered except where:

a. the email was a commercial electronic message within the meaning of the SPAM Act 2003 (Commonwealth);
b. the content of the email or any attachment to the email would or might have resulted in an unauthorised interference with, damage to or operation of a computer or computer network operated by the employer or of any program run by or data stored on such a computer or computer network;
c. the email or any attachment to the email would be regarded by a reasonable person as being, in all circumstances menacing, harassing or offensive; or
d. the University was not aware (and could not reasonably be expected to be aware) of the identity of the employee who sent the email or that the email was sent by an employee.

(78) The University will not prevent delivery of an email or access to online content if:

a. the email was sent by or on behalf of an industrial organisation or employees or an officer of such an organisation; or
b. the online content or email contains information relating to industrial matters.

(79) The University has a legitimate right to capture and inspect any data stored or transmitted on the University's IT facilities and services and personally owned devices including data of a private or personal nature (regardless of data ownership), when investigating system problems or potential security violations, and to maintain system security and integrity, maintain business continuity, and prevent, detect, or minimise unacceptable behaviour on that facility. Such data will not be released to persons within or outside of the University, except in response to:

a. permission from the user;
b. a request from a Senior Executive, Executive Dean or Director/Chief Officer to investigate a potential breach of policy;
c. circumstances where it is deemed appropriate by the University for the purpose of business continuity, a request from a Senior Executive, Executive Dean or Director/Chief Officer,
d. circumstances considered by the University to be sufficiently exceptional to warrant the release of the data;
e. circumstances where it is deemed appropriate by the University in order to uphold the statutory rights of individuals in matters such as privacy, copyright, workplace health and safety, equal employment opportunity, harassment and discrimination;
f. a proper request from an appropriate law-enforcement officer investigating an apparently illegal act, including a court order; or
g. where authorised or permitted under a relevant law or statute.
h. A third party that has been contractually engaged by the University to provide IT related services.

(80) Access to data will only be granted following a request from the Senior Executive, Executive Dean or Director/Chief Officer, made in writing, and approved by the Chief Information Digital Officer, or delegated person.

(81) Access to any data will always be via network or systems administrators, or via persons nominated by the Chief Information Digital Officer or delegated person. The University's policy and statutory legislation relating to privacy will be upheld in all cases.

Section 6 - Administration and Implementation

Compliance

(82) This compliance section is relevant and enforceable across all IT policy documents.

(83) The University treats misuse of its IT facilities and services seriously. Violations of the conditions of use of IT facilities and services may result in temporary or indefinite withdrawal of access, disciplinary action under the University's or relevant entity's discipline procedures, and/or demand for reimbursement to the University.

(84) Allegations of IT misconduct by students will be dealt with under the Student Conduct Rules. The Chief Operating Officer and Vice-President Operations or their nominee will be the Primary Investigation Officer for dealing with allegations of IT misconduct by students. Detailed investigation procedures and the penalties that may be applied to students engaging in IT misconduct can be found in the Student Conduct Rules.

(85) In the case of misuse of IT facilities and services by a staff member of a controlled entity or affiliate, a user's access will be withdrawn following a written request from the relevant Director/CEO of the controlled entity or affiliate. Access may also be withdrawn by IMTS in response to a suspected policy violation.

(86) In the case of misuse of IT facilities and services by a Staff member of the University, a user's access will be withdrawn following a written request from the relevant Senior Executive, Executive Dean or Director. Access may also be withdrawn by IMTS in response to a suspected policy violation.

(87) Any user whose access has been withdrawn may request reconsideration of the decision by the Chief Information Digital Officer who shall consider the withdrawal in consultation with the relevant controlled entity or affiliate. Following this, the Chief Information Digital Officer shall confirm the withdrawal or reinstate access.

(88) Misuse or unauthorised use of University IT facilities and services may constitute an offence under the Crimes Act 1914 (Commonwealth) and/or other relevant State or Commonwealth legislation. Nothing in this Policy may be taken as in any way diminishing or removing a person's obligations to comply with the law, or their liability to prosecution and punishment under law.

(89) Users are encouraged to report any misuse and any reports will be treated as confidential.

Section 7 - Roles and Responsibilities

(90) Roles and responsibilities are as detailed throughout this Policy, the Cyber Security Policy, and the Data Governance Procedure.

Section 8 - Definitions

Word/Term	Definition (with examples if required)
Computer Surveillance	Means surveillance, including by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, local or hard drive, public network, internet and email and other electronic technologies).
Crisis	An emergency or series of incidents that seriously threatens the University's people, assets, continuity (>72hrs), the environment, its long-term prospects and / or reputation and requires strategic management of consequences.
Data Governance	The specification of decision rights and an accountability framework to ensure the appropriate behaviour in the valuation, creation, consumption, and control of data.

Word/Term	Definition (with examples if required)
device	Any device that is provided to University staff, or required to maintain and provide services, and paid for by the University for the purposes of fulfilling individual work requirements. This includes those devices loaned to students for study purposes.
Email Account	An Email Account issued to a User to use whilst employed at or enrolled at the University of Wollongong.
Emergency	An event or series of events that arises from internal or external sources, requires an immediate response, poses risk to life, property, or continuity of operations (>1day) and / or requires strategic management of consequences.
Enterprise Storage	Storage provided through IMTS that is protected from data loss; whether that storage be on premise or cloud based.
IT facilities and services	Information Technology facilities operated by or on behalf of the University. This includes services and systems and associated computing hardware and software used for the communication, processing, and storage of information.
IMTS	Information Management & Technology Services at the University of Wollongong.
Staff	All people employed by the University including conjoint appointments, whether on continuing, permanent, fixed term, casual or cadet or traineeship basis.
Student	A person formally enrolled in a course at the University of Wollongong.
University	University of Wollongong and controlled entities.
User	A person assigned a user account by the University or a person who is otherwise authorised to use University IT facilities and services.
User account	An identity assigned to a User, with an associated username, for the purpose of accessing IT facilities and services that require authentication by the user. Also referred to as account throughout this document.

Status and Details

Status	Current
Effective Date	13th December 2023
Review Date	13th December 2028
Approval Authority	University Council
Approval Date	13th December 2023
Expiry Date	Not Applicable
Responsible Executive	Adam Malouf Chief Operating Officer and Vice-President Operations
Responsible Officer	Ray Coury Chief Information Digital Officer
Enquiries Contact	Information Management and Technology Services +61 2 4221 3000