UNIVERSITY
OF WOLLONGONG
AUSTRALIA

IT ACCEPTABLE USE POLICY

Date first approved: 1 July 2004	**Date of effect:** 1 July 2004	**Date last amended:** (refer Version Control Table) 9 February 2021	**Date of Next Review:** August 2024
First Approved by:	Vice-Chancellor		
Custodian title & e-mail address:	Senior Manager Client Services, IMTS imts-admin@uow.edu.au		
Author:	Cyber Security Manager, Infrastructure, IMTS Senior Manager Client Services, IMTS		
Responsible Division & Unit:	Information Management & Technology Services (IMTS)		
Supporting documents, procedures & forms of this policy:	Bullying Prevention Policy Copyright Policy Cyber Security Policy Data Governance Procedure Data Handling Guidelines Fraud and Corruption Prevention Policy IT User Account Management Procedures Privacy Policy Purchasing and Procurement Policy Records Management Policy Research Data Management Policy Secondary Employment Policy Sexual Harassment Prevention Policy Student Conduct Rules Telephone and Mobile Use Policy Travelling Overseas with Devices Procedures University Code of Conduct University Privacy Statement & Policy		
Relevant Legislation & External Documents:	*Crimes Act 1914* (Commonwealth) *Workplace Surveillance Act 2005* (NSW) *Criminal Code Act 1995* (Commonwealth) *SPAM Act 2003* (Commonwealth) *Copyright Act 1968* (Commonwealth) *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Commonwealth) Microsoft Product Terms and Online Services Terms (OST)		
Audience:	Public		

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Submit your feedback on this policy document using the Policy Feedback Facility.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Contents

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

1 Purpose of Policy

1. The University of Wollongong 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 policies 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.

2 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.
Device	Any Device that is provided to University staff and paid for by the University for the purposes of fulfilling individual work requirements.
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.

3 Application & Scope

1. 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 applications, web services, cloud services and similar resources. 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.
2. Users must accept and comply with University IT policies as a condition of use. This policy is designed to allow legitimate and optimal use of IT Facilities and Services.

4 Policy Principles

1. IT Facilities and Services are provided to Users to conduct teaching, learning, research and administrative pursuits.
2. 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.

Authorised Use, Access and Authentication

3. 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.
4. User Account creation and management is governed by the IT User Account Management Procedures.
5. Many IT Facilities and Services require authentication in order to access, and some require Multi Factor Authentication (MFA). Access is often further controlled based on roles, which are linked with the username of a User Account.
6. Some IT Facilities and Services are provided only for specific functions and may only be used by specifically authorised Users.
7. Users must use IT Facilities and Services only in the manner intended for their role.
8. Users must not share their User Account or password or other authentication credential. 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.

9. Users must set up the self-service password reset capability to enable themselves to reset a forgotten or expired password.
10. Users are discouraged from recording passwords on paper. A secure password management system is recommended if needed.

Security

11. 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 University Staff.
12. For new Staff, Cyber Security Awareness Training is mandatory as part of their onboarding and probation requirements.
13. Managed computers that are compromised will be reset to the standard image and software reinstalled by IMTS support staff.
14. All software on devices must be kept up to date to ensure known security vulnerabilities are fixed.
15. All devices must have security features such as password protection, firewall and anti-virus/anti-malware enabled where available;
16. 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 a website or entering private data, the security padlock and the legitimacy of the site address should be checked; 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.
17. 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.
18. Access to a User Account may be temporarily suspended if the account is suspected to be compromised and is posing an unacceptable risk.
19. Users must not give means to a third-party to access IT Facilities and Services without approval from the IMTS Security Team.
20. From time to time, 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 websites 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

21. 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.

22. 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

d. deliberate unauthorised access to IT Facilities or Services.

Using Devices and Equipment

23. Users should exercise care when using IT equipment. Users will be held responsible for cost of repair if damage is caused 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.

24. IT Facilities and Services must not be tampered with or moved without authorisation.

25. 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.

26. 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

27. 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 Acceptable Use 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.

Cloud Computing & External IT Services

28. Procurement of externally hosted IT services must comply with the Purchasing and Procurement Policy.
29. 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

30. Students are not allowed to install, attempt to install, copy, or download any type of software onto IT Facilities and Services, unless the student is in an IT Laboratory specifically setup for the purpose of studying an IT related discipline where:
    a. installation of software is required as part of the coursework;
    b. there is proof the software license belongs to the University; or
    c. the University has given their authorisation.
31. 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

32. The IT Facilities and Services are provided to support the University's teaching, research, administrative and services purposes.
33. 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 such 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.
34. 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

35. The University provides all Users with an email account.
36. All Users allocated an Office365 account must abide by the terms and conditions as outlined by Microsoft under the Product Terms and Online Services Terms (OST).
37. There are limits to the size of email items and the amount of email retained on servers, these may change from time to time.
38. There are limits to Internet data and bandwidth use, including web browsing activity, these may change from time to time.

39. The University may block or re-direct incoming email if they are deemed to be harassing or offensive to the recipient.

Telephones and Mobile Devices

40. The use of telephones and mobile Devices must comply with this policy and with the Telephone and Mobile Device Use Policy.

Data Governance

41. 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.
42. 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

43. Users are responsible for appropriately handling University data and must comply with relevant University policies such as the Privacy Policy, Intellectual Property Policy, Records Management Policy, Research Data Management Policy, Travelling Overseas with Devices Procedures, Data Handling Guidelines, and Data Governance Procedure.
44. Collection, access authorisation, and use of data must be underpinned by a relevant business need.
45. Responsibilities for providing access to data are outlined in the Data Governance Procedure and Delegations of Authority Policy.
46. Technical controls (e.g. file permissions and authentication) must be used to restrict access to authorised Users only.
47. University data assets, as defined in the Data Governance Procedure, must be assigned a level of security classification to ensure appropriate handling and protection.
48. The Data Handling Guidelines provide best practice guidance on how to protect and handle data based on security classification of its data assets.
49. 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

50. 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.
51. 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.
52. All University data must be primarily stored (or have a current copy stored) on enterprise storage provided through IMTS.
53. University data must not be stored on external portable storage, personally owned devices, personal cloud storage or personal email accounts.

54. Data defined as 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.
55. 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.
56. 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

57. 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.
58. 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 will enforce controls within the institution to prevent the copying or use of unauthorised music, videos, and software. This includes effective measures to verify compliance with these standards.

Dealings in Copyright Protected Material for Teaching or Research

59. 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).
60. Staff and students may also be able to copy limited portions of material under the 'fair dealing' provisions of the Copyright Act, 1968 (Commonwealth).
61. 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) see http://www.library.uow.edu.au/copyright/index.html

Privacy

62. 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 http://www.uow.edu.au/about/privacy/index.html
63. User's names and usernames will be listed in directories accessible to other Users for the purpose of enabling collaboration.
64. 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.
65. When using a multi-user system, Users must be aware that many of the activities undertaken may be visible to other Users.
66. 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 at least 2 years.

67. Authorised IT staff may incidentally observe data during the course of their duties.
68. 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

69. 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.
70. The University is committed to meeting its statutory obligations under the Workplace Surveillance Act 2005 (NSW) and this IT Acceptable Use Policy represents formal notification to Users about activities of the University that fall within the definition of Computer Surveillance.
71. 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.
72. 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.
73. 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; or
    c. access to software applications.
74. 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.

75. The University will not prevent delivery of an email or access to a website merely because:

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 website or email contains information relating to industrial matters.

76. 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 the Senior Executive, Executive Dean or Director 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 the Senior Executive, Executive Dean or Director,

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.

77. Access to data will only be granted following a request from the Senior Executive, Executive Dean or Director, made in writing and approved by the Director, IMTS or delegated persons.

78. Access to any data will always be via network or systems administrators, or via persons nominated by the Director, IMTS or delegated persons. The University's policy and statutory legislation relating to privacy will be upheld in all cases.

5 Administration and Implementation

Compliance

1. This compliance section is relevant and enforceable across all IT Policies.
2. 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.
3. Allegations of IT misconduct by students will be dealt with under the Student Conduct Rules. The Chief Operating Officer 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.
4. 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.
5. 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.
6. Any User whose access has been withdrawn may request reconsideration of the decision by the Director, IMTS who shall consider the withdrawal in consultation with the relevant controlled entity or affiliate. Following this, the Director, IMTS shall confirm the withdrawal or reinstate access.
7. 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.
8. Users are encouraged to report any misuse and any reports will be treated as confidential.

6 Roles and Responsibilities

1. Roles and Responsibilities are as detailed throughout this Policy, the Cyber Security Policy, and the Data Governance Procedure.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

7 Version Control and Change History

Version Control	Date Effective	Approved By	Amendment
1	1 July 2004	Vice-Chancellor	Policy converted into new ITS policy format. Addition of point re subverting restriction or accounting controls in Section 4 (point 8) Revised compliance statement to conform to the new Rules for Student Conduct. Compliance section under Administration and Implementation changed to include a reference to reimbursement to the University. Improved links to other policies Revised software and electronic materials section in line with the Music, Video and Software Piracy Policy. Completed the "Rules Governing the Use of IT Facilities" as an appendix to this policy. These are an extraction of the adopted IT policies and replace the now obsolete "Rules governing the use of University computer facilities". Removed appendix for email etiquette and rules governing the use of computer laboratories from this document.
3	1 September 2004	Vice-Chancellor	ITPAC and IT Forum approved version
4	15 November 2005	Vice-Chancellor	Included p2p example under General Principles Point 8.
5	6 May 2009	Vice-Principal (Administration)	Migrated to UOW Policy Template as per Policy Directory Refresh Renamed the Rules Governing the Use of It Facilities as "Requirements Governing the Use of IT Facilities."
6	9 March 2010	Vice-Principal (Administration)	Future review date identified in accordance with Standard on UOW Policy
7	19 March 2013	Finance and Resources Committee	Revised and updated policies approved by Finance and Resources Committee.
8	4 November 2013	Chief Administrative Officer	Updated to reflect title change from University Librarian to Director, Library Services.
9	30 January 2014	Vice-Chancellor (VCAG)	Updated University nomenclature
10	9 December 2016	University Council	Major review of IT Policy suite
11	1 May 2020	Chief Operating Officer	Administrative amendment to update Senior Executive titles.
12	21 August 2020	Vice-Chancellor	Scheduled review of IT policy suite resulting in minor amendments,
13	9 February 2021	Vice-Chancellor	Minor Amendments to reflect introduction of Data Governance Procedure and Data Handling Guidelines.
14	2 November 2022	Vice-Chancellor	Minor changes to Section 4.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA