Acceptable Use of UNSW Information and Communication Technology (ICT) Resources Policy

Version	Approved by	Approval date	Effective date	Next review
2.2	President and Vice-Chancellor	10 May 2021	10 May 2021	

Policy Statement	
Purpose	This policy informs users of University ICT resources of their rights and responsibilities; and of the University's requirement that its ICT resources are used in a legal, ethical and responsible manner. This policy is supported by the *Acceptable Use of Information and Communication Technology Resources Procedures* which is intended to ensure a clear and consistent understanding and implementation of this policy. The policy supports the *UNSW Code of Conduct*, which sets out the general rules of conduct for staff of the University and the UNSW *Student Code of Conduct*, which sets out the general rules of conduct for students.
Scope	This policy applies to **all** users of University ICT resources – including (but not limited to) staff (including casuals), students, consultants and contractors, third parties, agency staff, alumni, associates and honoraries, conjoint appointments and visitors to the University. This Policy applies to use of UNSW ICT and ICT resources **at all times**, regardless of whether such use occurs during business hours or on UNSW premises and applies to anyone connecting personally-owned equipment (e.g. laptops) to the University network. This Policy also *applies to the use of information* that may be accessed via the University's ICT resources.
Policy Provisions	

1. Preamble

Information and communications technology (ICT) is of critical importance to the University in the support of academic enquiry and research; teaching and learning; core business activities and communications. In recognition of this, UNSW provides computing, email, Internet and communication facilities to its staff and students for the purposes of research, teaching and learning; and to support the administration of the University.

2. Policy Statement

The conditions of use for UNSW information and communication technology resources are stated below. For an extension on each of the sections below, refer to the *Acceptable Use of Information and Communication Technology Resources Procedure*, which forms part of this policy. The key principles, and consequences of breaching this policy, are:

2.1. Provision of ICT Resources

The University recognises the importance of computing and communication technologies and will provide access to ICT resources for its staff, students and other authorised users, for the purposes of research, teaching, learning and administration, and in accordance with need and available resources.

2.2. Legal, Ethical and Responsible Use of ICT Resources

The University requires users to use ICT and ICT resources in a legal, ethical and responsible manner. Users of University ICT resources must be aware that use of these facilities is subject to State and Federal laws that apply to communications and to the use of computers, as well as any other relevant laws and UNSW policy. This includes (but is not limited to) copyright, intellectual property, breach of

confidence, defamation, privacy, contempt of court, harassment, vilification and anti-discrimination legislation, workplace surveillance, the creation of contractual obligations, civil and criminal laws.

The University's ICT resources must not be used to copy, download, store or transmit material, which infringes copyright, such as music files, movies, videos etc. In addition, the University's ICT resources must not be used for unauthorised commercial activities or unauthorised personal gain and must not cause loss of service, or risk loss of reputation to the University.

Limited incidental personal use of ICT resources is allowed, subject to the conditions of use stated in the *Acceptable Use of Information and Communication Technology Resources Procedure*. In addition, users should be aware that some third party applications licensed to the University (e.g. some of the large searchable databases available through the Library) have their own terms and conditions, which may apply over and above this policy.

2.3. Monitoring usage of ICT and ICT Resources

The University will take reasonable precautions to protect the security and privacy of its users' ICT accounts, but users should be aware that normal operation and maintenance of systems includes backup, logging of activity and monitoring of general usage patterns.

In addition, the University may monitor individual usage and records in accordance with this Policy.

Each person who uses ICT (e.g. computers, lap-tops, blackberries, iPhones, iPads or other tablet devices etc) and ICT resources (e.g. networks, hardware, software etc) should be aware that, in accordance with this Policy, UNSW monitors usage on a continuing and ongoing basis.

The technology supporting ICT and ICT resources involves recording, back-up and monitoring of all usage (including emails, Internet, hard drives, networks etc) for technology and data security purposes (such as system back up, network performance monitoring, software license monitoring, computer asset tracking etc).

UNSW may also monitor and access a user's individual records and usage where it has a reasonable basis to do so, provided that UNSW will, at all times, comply with applicable legislation. Information obtained may include personal information of the individual, which will be managed in accordance with privacy legislation and the University's *Privacy Policy*.

In addition the provisions below are applicable to employees of UNSW.

2.3.1. Workplace Surveillance Act (NSW)

The *Workplace Surveillance Act* (NSW) requires that the University have a policy, which sets out the specific basis upon which the University may monitor the IT usage of University employees. This next section is intended to meet the requirements of the *Workplace Surveillance Act* (NSW).

UNSW may monitor and access individual records (such as email records, internet usage, network drives and hard drives etc.) in limited circumstances. In doing so, UNSW is committed to balancing an employee's right to privacy with the legitimate protection and proper usage of UNSW resources. UNSW also recognises that the nature of University work means that an employee may use these resources for a broad range of legitimate purposes (consistent with the principles of academic freedom). UNSW monitors individual records for the limited purposes of ensuring security and to meet legitimate business needs.

Consistent with these purposes, UNSW will normally only access an employee's records in the following circumstances:

1. When an employee is unexpectedly absent from work (for example, on sick leave or annual leave) and access is required for legitimate business purposes (for example, work continuity) or occupational health and safety reasons (for example, where there are reasonable concerns about the individual's health and safety).

2. When UNSW reasonably suspects that an individual(s) is not complying with this Policy, other UNSW policies or procedures (eg *Code of Conduct*), or legislation.
3. For use in legal proceedings or as required by law (eg to comply with a Notice to Produce or subpoena).
4. For IT security purposes (eg to protect networks or data stored on the network).

Consistent with this approach, access to IT records, including any conditions prescribed, will only be provided to an appropriately senior staff member where approval has been obtained from the Chief Technology & Infrastructure Officer and either:

- Director, Chief Human Resources Officer, or their nominee in circumstances of absence, (where staff are involved); or
- Deputy Vice-Chancellor Academic and Student Life, or their nominee in circumstances of absence (where students are involved); or
- Deputy Vice-Chancellor Planning and Assurance, or their nominee in circumstances of absence.

As an exception, no co-signature is required where the process of giving approval risks disclosing the identity of a whistleblower. In this circumstance, the approver would be the Deputy Vice-Chancellor Planning and Assurance and the requestor would need to justify in writing why a co-signature risks identifying the whistleblower. Where an approver conflict of interest exists, alternative approval will be sought from the President & Vice-Chancellor or an appropriate member of Council.

2.4. Academic Freedom and freedom of expression

The University values and respects the principles of academic freedom. It values the diversity of cultures, ideologies and perspectives within its community and is respectful of freedom of expression. However these privileges must be exercised responsibly and the University will not tolerate any conduct, which breaches the A*cademic Freedom and Freedom of Speech Code of Conduct, Code of Conduct*, *Student Code of Conduct*, policies, procedures or legislation.

For more information on the conditions of use, refer to Section 5, Breaching the conditions of use, in the *Acceptable Use of Information and Communication Technology (ICT) Resources Procedure.*

3. Legal & Policy Framework

It should be noted that student misuse of ICT resources could also be regarded as Academic Misconduct (under the *Student Code of Conduct* and associated *Student Misconduct Procedure*) and that the UNSW Chief Technology & Infrastructure Officer can impose financial penalties.

Users of University ICT resources must be aware that the use of these facilities is subject to State and Federal laws that apply to communications and to the use of computers as well as any other relevant laws and UNSW policy. This includes (but is not limited to) copyright, breach of confidence, defamation, privacy, contempt of court, harassment, vilification and anti-discrimination legislation, the creation of contractual obligations and civil and criminal laws.

In conjunction with this policy all staff and affiliates are referred to the University's *Code of Conduct* and Academic staff to the UNSW *Paid Outside Work by Academic Staff Policy* with regard to the use of University resources for private professional practice. Students should refer to the *Student Code of Conduct* and *Student Misconduct Procedure*.

In addition, users should be aware that some third party applications licensed to the University (e.g. some of the large searchable databases available through the library) have their own Terms and Conditions, which may apply over and above this policy.

Accountabilities	
Responsible Officer	Chief Technology & Infrastructure Officer
Contact Officer	Chief Information Security Officer (CISO) – Cyber Security
Supporting Information	
Legislative Compliance	This Policy supports the University's compliance with the following legislation: • *Copyright Act 1968* (Cth) • *Corporations Act 2001* (Cth) • *Public Interest Disclosures Act 1994* (NSW) • *Privacy and Personal Information Protection Act 1998* (NSW) • *Workplace Surveillance Act 2005* (NSW) as well as laws relating to (but is not limited to) breach of confidence, defamation, contempt of court, harassment, vilification and discrimination, the creation of contractual obligations and civil and criminal offences.
Supporting Documents	Acceptable Use of UNSW Information and Communication (ICT) Resources Procedure
Related Documents	Academic Freedom and Freedom of Speech Code of Conduct Code of Conduct Student Code of Conduct Student Misconduct Procedure IT Security Policy Report Wrongdoing Policy Report Wrongdoing Procedure Research Code of Conduct Research Misconduct Procedure
Superseded Documents	Acceptable Use of UNSW Information and Communication Technology (ICT) Resources Policy v2.1
File Number	2021/018579
Definitions and Acronyms	
Refer to the *Acceptable Use of UNSW Information and Communication (ICT) Resources Procedure*	

Revision History

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Vice-Chancellor	November 2006	1 March 2007	
1.1	Head, Governance Support	18 February 2010	18 February 2010	Section 1, 2, 6.1, 6.1.1(a), 6.1.1(c)
2.0	President and Vice-Chancellor	6 June 2013	30 June 2013	Full review; additional requirements in Section 2.3
2.1	Administrative update by the Director of Governance	17 October 2016	17 October 2016	Section 1; 2; 2.2; 2.3; 2.3.1; 2.4 and 3.
2.2	President and Vice-Chancellor	10 May 2021	10 May 2021	Section 2.3.1 and 2.4 amended. Administrative updates to document and position titles and URLs.