



Version	Approved by	Approval date	Effective date	Next full review
3.0		XX Month Year	XX Month Year	
Policy Statement				
Purpose	This policy: a) sets out the principles for ensuring UNSW Information Resources (systems, infrastructure, UNSW-wide IT assets) are used ethically and responsibly. b) sets out the conditions for personal use of UNSW Information Resources. c) informs users of UNSW Information Resources of their responsibilities and the penalties for misuse. d) establishes compliance requirements for users of UNSW Information Resources. e) establishes requirements for reporting cyber security events. f) reflects UNSW's values.			
Scope	This policy applies to all users of UNSW Information Resources, including but not limited to staff (including casuals), students, consultants, contractors, third parties, agency staff, alumni, associates and honoraries, conjoint appointments, affiliates, collaborative researchers, and visitors to UNSW including any use before, during and after any formal relationship exists.			
Policy Provisions				

1. Compliance

1.1. General

- (1) UNSW requires its Information Resources to be used legally, ethically, and responsibly.
- (2) Users of UNSW Information Resources must comply with:
 - a. applicable laws, including (but not limited to) copyright, intellectual property, breach of confidence, defamation, privacy, contempt of court, harassment and cyber stalking, vilification and anti-discrimination legislation, and workplace surveillance legislation.
 - b. UNSW policies and procedures.
 - c. the UNSW Cyber Security Standards.

(3) Users must not use UNSW Information Resources to:

- a. harass, stalk, menace, defame, vilify, or unlawfully discriminate against any other person. Refer to the *Workplace Bullying Policy*.
- b. collect, use or disclose personal information except in accordance with the *UNSW Privacy Policy*.
- c. copy, download, store or transmit material which infringes the intellectual property of any other party. Refer to the *Intellectual Property Policy*.
- d. transmit material in contravention of the *Spam Act 2003* (Cth).
- e. represent or create the impression of representing UNSW unless explicitly authorised to do so.
- f. represent another person or claim to represent another person unless explicitly authorised.
- g. otherwise cause loss or harm to the reputation of UNSW.

1.2. Academic Freedom and Freedom of Expression

UNSW 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 UNSW manages any conduct, which breaches relevant policies, standards or legislation including the *Academic Freedom and Freedom of Speech Code of Conduct*, *Staff Code of Conduct*, *Student Code of Conduct* or *Research Code of Conduct*, in accordance with the relevant procedure or enterprise agreement.

2. User Responsibilities and Prohibitions

2.1. Responsibilities

- (1) Users are responsible for all activities originating from their UNSW accounts or other UNSW accounts that they use, as well as any digital information they store, process, or transmit using, or while connected to, a UNSW Information Resource.
- (2) Users must take all reasonable steps to protect UNSW Information Resources from physical or digital theft, damage, or unauthorised use.
- (3) Users, other than students with no other role within UNSW, must complete UNSW assigned cyber security awareness training.
- (4) Users must only store, process or transmit UNSW digital information in accordance with the *Data Classification Standard* and *Cyber Security Standard - Data Security*.

2.2. Prohibitions

UNSW recognises that the nature of university work, study and research means that a user may use Information Resources for a broad range of legitimate purposes (consistent with the principles of academic freedom), however:

- (1) Users must not:
 - a. use another person's account.
 - b. share their password or other authentication factor with another person or third party.
 - c. assist or permit the use of UNSW Information Resources by an unauthorised person.
 - d. attempt to gain unauthorised access to UNSW Information Resources.
 - e. use UNSW Information Resources, or personal devices, to maliciously compromise the confidentiality, integrity, availability or privacy of UNSW Information Resources or UNSW digital information.

- f. use UNSW Information Resources to access, display, store, copy, process, transmit or provide prohibited or restricted material, other than in accordance with [Section 3](#).
 - g. intentionally circumvent identity controls or other cyber security controls for a malicious purpose.
 - h. test, bypass, deactivate or modify the function of any cyber security control (including an operating system), except:
 - i. for research or teaching purposes; and
 - ii. with express written approval of the Head of School or equivalent; and
 - iii. in an isolated testing environment or isolated network.
 - i. knowingly install or use malicious software, except:
 - i. for research or teaching purposes; and
 - ii. with express written approval of the Head of School or equivalent; and
 - iii. in an isolated testing environment or isolated network.
 - j. connect an end-of-life, end-of-support, or intentionally compromised device to UNSW Information Resources except:
 - i. for research or teaching purposes; and
 - ii. with express written approval of the Head of School or equivalent; and
 - iii. in an isolated testing environment or isolated network.
- (2) Users must not use UNSW Information Resources to generate or process (mine) crypto currency except for research or teaching purposes, and with the express written approval of the Head of School or equivalent. The use of a crypto currency wallet in a payment transaction is not considered processing for the purposes of this policy.
- (3) Staff and students must not use UNSW Information Resources for financial or commercial gain for themselves or any third party. UNSW Information Resources must not be leased, lent, or otherwise made available to third parties for personal profit. Staff should refer to the UNSW *Staff Code of Conduct*. Academic staff should also refer to the UNSW *Paid Outside Work by Academic Staff Policy*.

3. Restricted and Prohibited Use

3.1. Prohibited and Restricted Material

- (1) Users must not access, display, store, copy, or transmit prohibited or restricted material on or using UNSW Information Resources except:
- a. for research or teaching purposes; and
 - i. in accordance with all laws, policies, procedures, and standards, including the *Research Code of Conduct*; and
 - ii. with human or animal ethics approval where appropriate; and
 - iii. with the express written approval of a relevant Deputy Vice-Chancellor (for prohibited material) or a Head of School or equivalent (for restricted material).
 - b. for the purpose or intention of investigation of a potential breach of a code of conduct, policy, procedure by the Conduct and Integrity Office or Human Resources.

4. Personal Use of University Information Resources

4.1. Limited Personal Use

- (1) UNSW provides access to UNSW Information Resources for users to perform legitimate University related work, research or studies and all usage must be consistent with that purpose.
- (2) Users are permitted limited and incidental personal use of UNSW Information Resources. This use:
 - a. must not directly or indirectly impose an unreasonable burden on any Information Resource, or burden UNSW with incremental costs.
 - b. must not unreasonably deny any other user access to any Information Resource.
 - c. must not contravene any law or University policy or procedure.
 - d. in the case of staff, must not interfere with the execution of their responsibilities.
- (3) Users should be aware that some third-party applications provided by UNSW have their own terms and conditions, which may apply additional limitations.
- (4) Users who store, process or transmit their own personal information as part of their personal use of a UNSW Information Resource, are responsible for deciding how that information is secured (e.g. encrypted) and backed up. UNSW is not responsible for ensuring the retention of personal data or providing such data to a user.
- (5) In conjunction with this policy all staff and affiliates are referred to the UNSW *Code of Conduct*, and Academic staff to the UNSW *Paid Outside Work by Academic Staff Policy* with regard to the use of UNSW resources for private professional practice. Students should refer to the *Student Code of Conduct* and *Student Misconduct Procedure*.

5. Personal Devices

5.1. Limitations

- (1) Users must only connect a personal device to a UNSW Information Service or UNSW Information Asset (including the UNSW network) in accordance with the Cyber Security Standards.
- (2) Users must not perform system administration tasks on any medium or high cyber security risk rated UNSW Information Resource (application or infrastructure), using a personal device.
- (3) UNSW does not guarantee that a personal device will be able to access or be compatible with all Information Resources.
- (4) All UNSW digital information must be stored in accordance with the *Cyber Security Standard – Data Security*.
- (5) UNSW reserves the right to access any UNSW digital information stored on personal devices in accordance with the privacy laws and this policy.

6. Terms of Use

- (1) UNSW will implement reasonable precautions to protect the security of UNSW Information Resources, however UNSW is not able to guarantee that UNSW Information Resources will always be available, secure, and confidential, or free from any defects, including malicious software.

- (2) UNSW accepts no responsibility for loss or damage (including consequential loss or damage or loss of data) arising from the use of UNSW Information Resources, or the maintenance and protection of UNSW Information Resources.
- (3) UNSW may take any necessary action in accordance with the UNSW Cyber Security Standards, to mitigate any threat to UNSW Information Resources, with or without prior notice.
- (4) UNSW at all times reserves the right (in accordance with Section 7) to:
 - a. limit or terminate the use of UNSW Information Resources, with or without notice.
 - b. view, copy, disclose or delete UNSW digital information stored, processed, or transmitted using UNSW Information Resources.
 - c. monitor or examine the security of any device connecting to UNSW Information Resources, to determine or address a cyber security threat to UNSW.
 - d. monitor, access, examine, take custody of, and retain any UNSW Information Resource.
- (5) Access to an Information Resource or storage, processing and transmitting of digital information (including email) may be delayed or prevented in the event of misuse or suspected misuse, or in the event of a security event or suspected event.
- (6) UNSW may at any time require a user to:
 - a. acknowledge in writing that they will abide by this policy.
 - b. complete relevant training in UNSW policies and procedures.

7. Monitoring and Surveillance of Information Resources

- (1) This policy sets out the basis on which UNSW may monitor usage of Information Resources in accordance with applicable laws and is a Notice of Surveillance under the *Workplace Surveillance Act 2005* (NSW).

7.1. Ownership of Digital Information and Right to Monitor

- (1) All digital information stored, processed, or transmitted using any UNSW Information Resource:
 - a. may be recorded and monitored on an ongoing and continuous basis, in accordance with the *Cyber Security Standards*.
 - b. may be subject to the *Government Information (Public Access) Act 2009* (NSW).
 - c. may be subject to the *Privacy and Personal Information Protection Act 1998*(NSW).
 - d. may be subject to the *Health Records and Information Privacy Act 2002* (NSW).
 - e. may be subject to the *State Records Act 1998* (NSW).
 - f. will remain in the custody and control of UNSW.
- (2) The technology supporting UNSW Information 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, intrusion detection, security incident management and forensics, software license monitoring, computer asset tracking etc). This may include personal drives or devices mapped to a UNSW Information Resource.
- (3) Digital information may be retained as long as required in accordance with relevant statutes, regulations, archival purposes and business needs. Refer to the *Data Retention Procedure – Home Drives, Office 365 & One Drive* for further information.

7.2. Privacy compliance and access to Information Resources

- (1) UNSW is committed to balancing all users right to privacy with the legitimate protection and proper usage of UNSW Information Resources. UNSW will take reasonable precautions to protect the privacy of users, however the use of UNSW Information Resources is not considered a private action or conduct.
- (2) Users should be aware that personal use of UNSW Information Resources may result in UNSW holding personal information about the user or others which may then be accessed and used by UNSW to ensure compliance with this, and other policies. This information will be managed in accordance with privacy legislation and the UNSW *Privacy Policy*.
- (3) UNSW must use personal information only for the purpose for which it was collected. To the extent that UNSW does collect personal information through scanning, monitoring, and accessing Information Resources including connected personal drives and devices:
 - a. scanning and monitoring of personal drives and devices mapped to a UNSW Information Asset will not unreasonably intrude into the personal affairs of individual staff or students.
 - b. any such information will only be used for assessing compliance with this policy, other UNSW policies or procedures, or legislation; or identifying and addressing security threats to UNSW Information Resources and will not be used for any other purpose.
 - c. Any inspection, access or examination of Information Resources must be in accordance with the *Cyber Security Standards*.
- (4) UNSW may access UNSW Information Resources and any other devices connecting to a UNSW Information Resources, including any personal information contained therein, in the following circumstances:

Circumstance	Approver
When required for legal proceedings or as required by law (e.g. to comply with a Notice to Produce or subpoena)	General Counsel, or their nominee
For cyber security purposes	Chief Information Officer, or their nominee
When UNSW reasonably suspects that an individual(s) is not complying with legislation, this policy and/or other UNSW codes, policies or procedures	Chief Information Officer, or their nominee; AND the relevant responsible officer for the policy.
When a staff member is absent from work 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),	Chief Human Resources Officer, or their nominee
When a student or researcher is absent from study or research 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),	Deputy Vice Chancellor Academic and Student Life, or their nominee
When an approver conflict of interest exists, or where confidentiality is required for a protected disclosure.	Deputy Vice-Chancellor Planning and Assurance, Vice-Chancellor and President, or an appropriate member of Council.

8. Reporting Cyber Security Events

- (1) Any person who identifies or suspects a cyber security event must report it as soon as possible to UNSW IT Service Centre.
- (2) Users must not:
 - a. Perform any action to manage or address a cyber security event unless authorised or explicitly instructed by the UNSW IT Service Centre or UNSW IT Cyber Security Team.
 - b. Disclose information relevant to any cyber security event other than in accordance with the UNSW Cyber Security Standards.
- (3) The loss, theft or damage to UNSW Information Assets must be reported at the earliest opportunity to UNSW Campus Security.

9. Misuse

- (1) In the event of misuse or suspected misuse of UNSW Information Resources (as determined by the Chief Information Security Officer, or their nominee), UNSW may:
 - a. withdraw or restrict a user's access to UNSW Information Resources.
 - b. commence disciplinary action:
 - i. for staff: disciplinary action in accordance with the UNSW *Code of Conduct* and the applicable *University of New South Wales Enterprise Agreement*, which may include termination of employment.
 - ii. for students: action for misconduct under the *Student Code of Conduct* and associated *Student Misconduct Procedure*, which may include exclusion from UNSW.
 - iii. for non-staff members, commensurate action, which may include termination or non-renewal of their appointment or contract.
 - c. apply financial penalties, as determined by the Chief Information Officer; and recorded in the *Schedule of Student Fines for Misuse of IT Resources*.
 - d. notify the Police or other relevant government authority.

Accountabilities	
Responsible Officer	Chief Information Officer
Contact Officer	Chief Information Security Officer (CISO)
Supporting Information	
Legislative Compliance	<p>This Policy supports UNSW's compliance with the following legislation:</p> <ul style="list-style-type: none"> • <i>Copyright Act 1968</i> (Cth) • <i>Corporations Act 2001</i> (Cth) • <i>Government Information (Public Access) Act 2009</i> (NSW) • <i>Health Records and Information Privacy Act 2002</i> (NSW) • <i>Privacy and Personal Information Protection Act 1998</i> (NSW) • <i>Public Interest Disclosures Act 1994</i> (NSW) • <i>Spam Act 2003</i> (Cth) • <i>State Records Act 1998</i> (NSW) • <i>Workplace Surveillance Act 2005</i> (NSW) <p>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.</p>
Supporting Documents	<p>Cyber Security Policy</p> <p>Cyber Security Standards</p> <p>Data Classification Standard</p> <p>Cyber Security Standard - Data Security</p>
Related Documents	<p>Data Governance Policy</p> <p>Report Wrongdoing Policy</p>
Superseded Documents	Acceptable Use of UNSW Information and Communications Technology (ICT) Resources Policy v2.2
File Number	[For Governance Use]

Definitions and Acronyms	
Cyber Security Control	means any management, operational or technical measure (including safeguards or countermeasures) put in place for cyber security.
Cyber Security Event	means an occurrence of an information resource state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.
Digital Information	means information that is in a digital or electronic form and is stored, processed or transmitted within an Information service or an Information Asset
Device	means Information Asset.
Intentionally Compromised Device	means a UNSW Information Asset or personal device that has been intentionally altered by the user or with the knowledge of the user, to introduce a security vulnerability or malicious code, or otherwise lack a cyber security control required under the Cybersecurity Standards.
Information	means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual.
Information Resource	means any Information Service, Information Asset or digital information.
Information Service	means any business or technology function provided by one or more Information Assets including but not limited to: (a) application systems (including software-as-a-service); and (b) Information infrastructure services such as operating systems, databases, voice and data telecommunications services, network services, media services, file and print services, and email services.
Information Asset	Means any hardware (including IoT devices), software, cloud-based services, communication devices, networks, that is stores, processes or transmits UNSW digital information.
Malicious Code	means software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an ICT Service or ICT Asset. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Misuse	means use of the UNSW Information Resources in contravention of any law or UNSW policy, procedure or standard.
Personal Device	means a non-UNSW owned or provided device that is used by an individual to access, store, process or transmit UNSW data or digital information. This includes desktops and laptop computers, personal digital assistants, tablets, smartphones, mobile PIN pads, radio communication devices, USB keys or any form of portable storage device.
Prohibited Material	means content, such as: (a) child exploitation material including child pornography or material that instructs, promotes or incites child abuse; (b) content that shows extreme sexual violence or materials that are overly violent; (c) materials that provoke the viewer into committing crimes and carrying out violent acts. This might be material that instructs, promotes or incites violent acts; (d) material that is vilificatory or instructs, promotes or incites discrimination; and (e) content that promotes terrorism or encourages terrorist acts.

Protected Disclosure	means a as defined in the <i>Report Wrongdoing Policy</i> .
Restricted Material	means content that is not prohibited but: (a) is obscene or pornographic and permitted by law; or (b) is material that instructs or promotes gambling. This includes sexually explicit material, media, art, and/or products, or anything else containing adult content such as online groups or forums that are sexually explicit in nature, sites that promote adult services such as video/telephone conferencing, escort services or strip clubs.
Security Vulnerability	means a weakness in the design, implementation or operation of an Information Asset, Information Service, system component or cyber security control, which allows an attacker (threat agent) to compromise confidentiality, integrity or availability.
UNSW Account	means the access to UNSW Information Resources provided to holders of a Z-Id, UNSW email address or other credential.
UNSW Digital Information	Means digital information that is owned by UNSW.
UNSW Information Asset	Means any Information Asset that is owned, leased, operated or managed by any UNSW organisational unit, or provided by any UNSW organisational unit to users.
UNSW Information Service	Means any Information Service that is owned, leased, operated or managed by any UNSW organisational unit, or provided by any UNSW organisational unit to users.
UNSW Information Resource	Means any Information Resource that is owned, leased, operated or managed by any UNSW organisational unit, or provided by any organisational unit to users.
User	Means a user of any UNSW Information Resource including but not limited to staff (including casuals), students, consultants, contractors, third parties, agency staff, alumni, associates and honoraries, conjoint appointments, affiliates, collaborative researchers, and visitors to the UNSW, including any use before, during and after any formal relationship exists.

Consultation Draft

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.
3.0	Vice-Chancellor			Full review

Consultation draft