3.1	Vice-Chancellor	23 August 2023	23 August 2023

Policy Statement

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 accountable for all activities originating from their personal UNSW accounts, or other UNSW accounts that they use, as well as any UNSW 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) Staff and affiliates 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 UNSW 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 any other person.

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 below.

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.

d. in the case of staff, must not interfere with the execution of their responsibilities.

(3) 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. Personal Devices

5.1. Limitations

(1) To protect the security of UNSW Digital Information, staff performing University duties using personal devices must ensure that these devices:

a. are password protected, or have an equivalent access restriction mechanism enabled, where available.

b. have malware protection enabled, where available.

c. are patched or updated in a timely manner.

d. are encrypted.

(2) Staff must report the loss or theft of a personal device containing UNSW Digital Information in accordance with Section 8 (1) below.

(3) UNSW does not guarantee that a personal device will be able to access, or be compatible with, all UNSW Information Resources.

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, 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 a UNSW Information Resource, or storage, processing and transmitting of UNSW 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 UNSW Information Resources

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

7.1. Ownership of UNSW Digital Information and Right to Monitor

(1) All UNSW 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 UNSW Cyber Security Standards.

b. may be subject to the *Government Information (Public Access) Act 20092 r0 699.58 Tf(0)-10(ormat)-9(i)5(o*

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 and any one of: - Chief Human Resources Officer - Director, Conduct & Integrity or - Chief Information Officer.
For cyber security purposes.	Chief Information Officer; or Director, Cyber Security and any one of: - General Counsel - Chief Human Resources Officer or - Director, Conduct & Integrity.
When UNSW reasonably suspects that an individual(s) is not complying with legislation or UNSW codes, policies or procedures.	General Counsel, and any one of: - Chief Human Resources Officer - Director, Conduct & Integrity or - Chief Information Officer.
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	