c. UNSW Cyber Security Standards.

1.3. Users must not use UNSW Information Resources to:

a. harass, stalk, menace, defame, vilify, or unlawfully discriminate against any other person. Refer to the *Bullying and Harassment in the Workplace Prevention and Management 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 (IP) Policy*.

d. transmit material in contravention of the *Spam Act 2003* (Cth).

e. represent or create the impression of representing UNSW

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:

for research or teaching purposes; and
with express written approval of the Head of School or equivalent; and
in an isolated testing environment or isolated network.

d. knowingly install or use malicious software, except:

for research or teaching purposes; and
with express written approval of the Head of School or equivalent; and
in an isolated testing environment or isolated network.

e. connect an end-of-life, end-of-support, or intentionally compromised device to UNSW Information Resources except:

for research or teaching purposes; and
with express written approval of the Head of School or equivalent; and
in an isolated testing environment or isolated network.

Any non-compliance with these prohibitions must be approved in accordance with the *Cyber Security Standard - Framework Exemption*, including a mandatory risk assessment and agreed compensating controls.

2.7. Excessive use of UNSW Information Resources (e.g. to generate or mine crypto currency) is not permitted, except for research or teaching purposes, and with the express written approval of the Head of School or equivalent.

2.8. Staff and students must not use UNSW Information Resources for:

a. financial or commercial gain for themselves or any third party.

b. private professional practice.

2.9. Staff should refer to the UNSW *Code of Conduct and Values*, the *Conflict of Interest Disclosure and Man1 526.15 m0 g0 G 0.0012 Tc[e.)]TJ 0.000008871 0 595 reW*nBF1 9.96 Tf 2e0 595.3cial008871 0 595.32 84.92 rc*

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 UNSW Information Resources

Limited Personal Use

4.1. 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.

4.2. 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 UNSW Information Resource, or burden UNSW with incremental costs.

b. must not unreasonably deny any other user access to any UNSW Information Resource.

c. must not contravene any law or UNSW policy or standard.

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

4.3. 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

Limitations

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

a. are password protected

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.

6.5. 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.

6.6. 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

7.1. 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).

Ownership of UNSW Digital Information and Right to Monitor

7.2. 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 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.

7.3. UNSW Digital Information may be retained for as long as required in accordance with relevant statutes, regulations, or for archival purposes and business needs. Refer to the *Data Retention Procedure – Home Drives, Office 365 & One Drive* for further information.

Privacy compliance and access to UNSW Information Resources

7.4. 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.

7.5. 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 applicable privacy legislation and the UNSW *Privacy Policy*.

7.6. 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 UNSW Information Resources including connected personal drives and devices:


UNSW
SYDNEY

End of Support (EOS)	means the supplier no longer sells, provides updates, or renews support contracts for the UNSW Information Resource.
Excessive Use	means

Security Vulnerability