Digital Technology Conditions of Use Policy

Section 1 - Audience and Scope

(1) This policy applies to all users and uses of digital assets owned, supplied and or managed by the University and controlled entities. Examples of the University's digital assets include but are not limited to:

a. computing and network infrastructure used to create, store, process, or transmit information assets or data;
b. network connectivity services providing access to the internet, resources on-campus, controlled entities, and partnering organisations;
c. information assets including information, records, knowledge, data, metadata, machine learning and artificial intelligence models;
d. computing hardware including computers and mobile devices, storage media, peripherals, and printers;
e. computer-mediated reality technology;
f. software provided or managed by the University;
g. communication and sharing platforms;
h. cloud services; and
i. digital control and surveillance systems.

Section 2 - Purpose

(2) The University provides digital technology solutions to enable teaching, learning, research and administration activities.

(3) The University has a responsibility to govern the use of its digital technologies including data, to protect its organisation, information assets and users from risks that could arise from their misuse.

(4) All users of the University's digital assets must be aware of this policy and are expected to:

a. recognise its importance and be familiar with its provisions;
b. understand and adhere to their responsibilities and obligations; and
c. comply with this Policy as a condition of using the University's digital technology.

(5) Any user who is unsure of the meaning of any terms or statements in this policy should seek advice by contacting DTS.

(6) This document should be read in conjunction with supporting policies and documents which include, but are not limited to:

a. Digital Security Policy;
b. Records Governance Policy;
c. Privacy Management Plan;
d. Privacy Policy;

e. Intellectual Property Policy;
f. Responsible Conduct of Research Policy;
g. Staff Code of Conduct;
h. Student Code of Conduct;
i. Outside Work Policy;
j. Information Security BYOD Policy;
k. Fraud and Corruption Framework;
l. Public Interest Disclosures Policy; and
m. Managing Cyber Threats While Travelling.

(7) Legislation relevant to this Policy includes but is not limited to:

a. Privacy and Personal Information Protection Act 1998;
b. Health Records Information Privacy Act 2002 (NSW);
c. Higher Education Support Act 2003;
d. Healthcare Identifiers Act 2010;
e. Privacy Act 1988 (Cth);
f. Copyright Act 1968;
g. Workplace Surveillance Act 2005 (NSW);
h. Spam Act 2003;
i. Industrial Relations Act 1996;
j. Government Information Public Access Act 2009;
k. Criminal Code 1995;
l. Online Safety Act 2021;
m. Surveillance Devices Act 2007 (NSW); and
n. State Records Act (1998).

Section 3 - General Principles

(8) Digital assets support the achievement of the University's objectives. The use and access to digital assets is subject to relevant state and federal laws and all relevant University policies, procedures and codes of conduct.

(9) The misuse of digital assets presents risks to the University and as such access is not provided unconditionally.

(10) Subject to delegated authority where relevant, the University reserves the right to:

a. grant, limit or withdraw access to its digital assets;
b. control the introduction, deployment, and ongoing management of digital technologies within the University's campuses, controlled entities, and cloud environments;
c. continuously monitor the use of digital technology within the University, controlled entities, and cloud environments;
d. view, modify, copy, move, delete or otherwise handle data and information assets where it is reasonably contemplated for the prevention of risk and authorised by law, irrespective of any ownership or other rights claimed over the data or information assets; and
e. carry out enforcement and consequence actions for any activity which contravenes this policy.

(11) The University accepts no responsibility for unavailability, loss, or damage of data or information arising from the

use of the University's digital assets.

(12) All users must comply with this policy with respect to digital assets. A failure to comply with this policy may result in:

a. for employees, disciplinary action taken under the Staff Code of Conduct, enterprise agreement, University policy and/or employment contract;
b. for service providers, may result in termination of any relevant contract with the University;
c. for all users (including those categories above), restriction or cancellation of access to the University's digital assets; and
d. for all users, where a failure to comply could also amount to criminal conduct, referral to the relevant external authority.

Section 4 - Conditions of Use

(13) All users of the University's digital assets must:

a. only access digital technology and data once authorised either through a University-provided identity (includes guest), University-provided account, or approval from the University;
b. only use the University's digital assets for authorised work, study or research, and limited personal use, unless by exception from the Chief Digital & Information Officer (CDIO) or their nominee;
c. only use the approved level of access;
d. ensure minimal personal use, and ensure personal use complies with all conditions of this policy and:
    i. does not interfere with University operations;
    ii. does not burden the University with additional costs; and
    iii. does not expose the University to intolerable risk;
e. exercise lawful, ethical, equitable, and appropriate behaviour while using digital assets;
f. exhibit care and due diligence to ensure the University's digital assets are protected from damage and cyber security threats;
g. ensure that the usage and characteristics of personal devices that interact with the University's digital assets meet all the applicable requirements of this Policy and all other relevant policies;
h. take responsibility for all activities originating from their University-issued identity or account, including all information sent, requested, solicited or viewed;
i. abide by any instructions given by the CDIO or their nominee in relation to the University's digital technology. Such instructions may be issued by notices displayed in the vicinity of computing facilities, by letter, by electronic communication, in person or otherwise;
j. immediately report actual or suspected breaches of this Policy to Digital Technology Solutions (DTS).

(14) Access to University digital assets may be suspended or removed by the CDIO, System Owner or other authorised nominee based on a period of inactivity by the user of no less than 90 days.

(15) Inappropriate and/or misuse use of the University's digital assets may be deemed misconduct and dealt with accordingly, including loss of access to digital assets.

(16) Inappropriate and/or misuse of the University's digital assets includes but is not limited to:

a. using digital assets:
    i. in a manner that is harassing, discriminatory, defamatory, vilifying, abusive, rude, insulting, threatening,

or obscene;

ii. in such a way as to cause embarrassment or loss of reputation to the University;

iii. to impersonate or falsify information about other persons;

iv. to create, access, store, process, or transmit pornographic or offensive material or any other content that is illegal or considreed by the Chief Digital & Information Officer to be immoral; other than with specific written approval from an authorised University Officer for research related purposes. Where an approval is granted, users must exercise caution, including the use of a secure storage location to avoid undue circulation or access to files;

v. in a manner that constitutes an infringement of copyright or infringes a person's moral rights;

vi. to collect, use, store or disclose personal information or health information in ways that breach the University's Privacy Management Plan;

vii. for unauthorised profit making or commercial activities;

viii. to distribute unsolicited and/or unapproved advertising materials on behalf of the University or from organisations that have no connection with the University or involvement in its activities;

ix. in a manner which is intended or likely to corrupt or damage data, software or hardware, either belonging to the University or to anyone else, whether inside or outside the University network;

x. to gain, or attempt to gain, unauthorised access to any computer service;

xi. to exploit vulnerabilities in systems or use any technology designed to locate such vulnerabilities or circumvent security systems;

xii. to perform or attempt to, create, install, or execute any form of malicious software;

xiii. for unauthorised cryptographic calculations, including crypto mining;

xiv. to eavesdrop or intercept the communication or transmission of data or information.

b. Facilitating or permitting unauthorised use of the University's digital assets.

c. Making unauthorised configuration changes to the University's digital assets.

d. Circumventing IT and cyber security controls, whether owned or managed by the University or any other party.

e. Uploading or submitting University data to unauthorised systems or organisations. Examples include but are not limited to unauthorised cloud storage or archival services, personal email services; and unauthorised artificial intelligence.

f. Avoiding surveillance of the use of the University's digital technology. This includes using virtual private networking (VPN), encryption, obfuscation, encapsulation, encoding, or any other means to avoid surveillance.

g. Using, deploying or otherwise introducing unauthorised applications, services, devices, network interconnectivity, or cloud services to the University's digital environment. This includes the use of applications and services listed in this Knowledge Base Article.

(17) Users under 18 must have parental or guardian permission to access the internet with their University-issued user identity or account.

(18) Users seeking to introduce or deploy digital technology within the University are required to seek authorisation from the CDIO or their nominee.

Section 5 - Monitoring of Use

(19) Any monitoring and audit activities performed under this policy will be subject to law or a legally binding agreement.

(20) The University will conduct lawful surveillance of its digital assets on a continuous and ongoing basis. For the purposes of the Workplace Surveillance Act 2005 (Cth), this policy constitutes written notice of the University's

computer surveillance of its employees.

(21) The University may audit, whether directly or via independent third parties, its digital assets:

a. used under the context of a University user or device identity, whether issued or managed by the University;
b. used in the pursuit of University related business, research, or teaching activities; and
c. used within the geographic boundaries of University land, subterrain, and airspace.

(22) Use of the University's digital assets deemed inconsistent with this Policy's general principles and conditions of use may be investigated by the University. Prior to commencement of an investigation, written approval by the Chief Digital & Information Officer is required.

(23) Computer surveillance may be carried out by the University by:

a. recording the detailed logs of all transactions and use by users of the University's digital assets;
b. accessing University email accounts, archives, backups or emails; even where the user has deleted an email, the University may still retain archived and/or backup copies of the email;
c. accessing files stored on network drives, computers or in cloud services to which the University has administrative access; even where the user has deleted a file, the University may still retain archived and/or backup copies of the file;
d. accessing University owned work computers, including computer security and event logs;
e. recording network traffic activity including internet usage (including sites and pages visited, files downloaded, video and audio files accessed and data input) and accessing these records;
f. accessing system and event logs and login activity relating to the University's digital assets;
g. monitoring on a continual basis, through manual analysis and automated correlation activities using the University's Security Information and Event Management (SIEM) solution; and
h. obtaining location data for users to validate identity when accessing the University's digital environment.

(24) Subject to requirements under law, University users acknowledge that as a result of this computer surveillance, the University may prevent, or cause to be prevented, delivery of an email sent to or by, or access to an internet website by, the user.

(25) As soon as reasonably practicable, the University will notify an employee where an email has not been delivered except where:

a. the email was a commercial electronic message within the meaning of the Spam Act 2003 (Cth);
b. the content or any attachment to an email would or might result in an unauthorised interference with, damage to or operation of, a computer or computer network of the University or any program run by or data stored on such a computer or computer network;
c. the email or any attachment would be regarded by a reasonable person as being (in all circumstances) harassing, menacing or offensive; or
d. the University is not aware (or could not reasonably be expected to be aware) of the identity of the employee that sent the email or that the email was sent by an employee.

(26) The University will not prevent the delivery of an email or access to a website merely because:

a. the email was sent by or on behalf of an industrial organisation of the employees or an officer of such an organisation; or
b. the website or email contains information relating to industrial matters (as defined in the Industrial Relations Act 1996 (NSW).

(27) Each user acknowledges that the University may be required to produce the records it has obtained (as a result of the monitoring it has undertaken in relation to its digital assets) as a result of a request authorised by law, for example, the Government Information (Public Access) Act 2009.

Section 6 - Exceptions

(28) Exceptions to this policy may be requested by a user in writing to the CDIO subject to any relevant delegation of authority. Exceptions will be assessed based on their risk and value to the University, and any compensating controls.

Section 7 - Roles and Responsibilities

(29) The CDIO is responsible for:

a. the development and maintenance of this policy;
b. ensuring that users are aware of this policy;
c. monitoring use of the University's digital assets;
d. compliance to this policy and related enforcement actions;
e. investigating and reporting the suspected breach of the Digital Technology Conditions of Use Policy.

(30) The System Owner or Information Owner or their nominee is responsible for granting and managing authorisation to use a digital asset. This includes assessing a user’s suitability for authorisation, and for granting and revoking authorisation within the bounds of the digital assets for which they are responsible.

Status and Details

Status	Current
Effective Date	1st May 2025
Review Date	1st May 2028
Approval Authority	Chief Digital & Information Officer
Approval Date	28th April 2025
Expiry Date	Not Applicable
Responsible Executive	David Toll Chief Operating Officer
Enquiries Contact	Information Security Team

Glossary Terms and Definitions

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"Commercial activities" - As defined in the University of Newcastle Act 1989.

"Controlled entity" - Has the same meaning as in section 16A of the University of Newcastle Act 1989.

"Law" - All applicable statutes, regulations, by-laws, ordinances or subordinate legislation in force from time to time anywhere in Australia, whether made by the Commonwealth, a State, a Territory or a local government and, where the context permits, includes the common law and equity.

"Personal information" - Has the same meaning as in the Privacy and Personal Information Protection Act 1998 (NSW).

"Disciplinary action" - When used in relation to staff of the University, this is as defined in the applicable and current Enterprise Bargaining Agreement, or the staff member's employment contract. When used in relation to students of the University, this refers to the range of penalties that may be applied under the Student Conduct Rule.

"Health information" - As defined in the Health Records and Information Privacy Act 2002, or any replacing legislation.

"Information asset" - A body of information, knowledge or data that is organised as a single entity and has value to the University.

"Information Owner" - A senior business, college or unit manager whom the University has authorised to collect, create, retain and maintain information within their assigned area of control.

"Officer" - Has the meaning given in the Corporations Act 2001 (Cth), or any replacing legislation.

"Research" - As defined in the Australian Code for the Responsible Conduct of Research, or any replacing Code or document.

"System Owner" - An authorised individual who has been allocated responsibility by the University and is held accountable for an ICT resource.

"Digital asset" - Means all or any information technology solution(s) (regardless of whether they are physical or software-based), and the facility(ies) that house them.