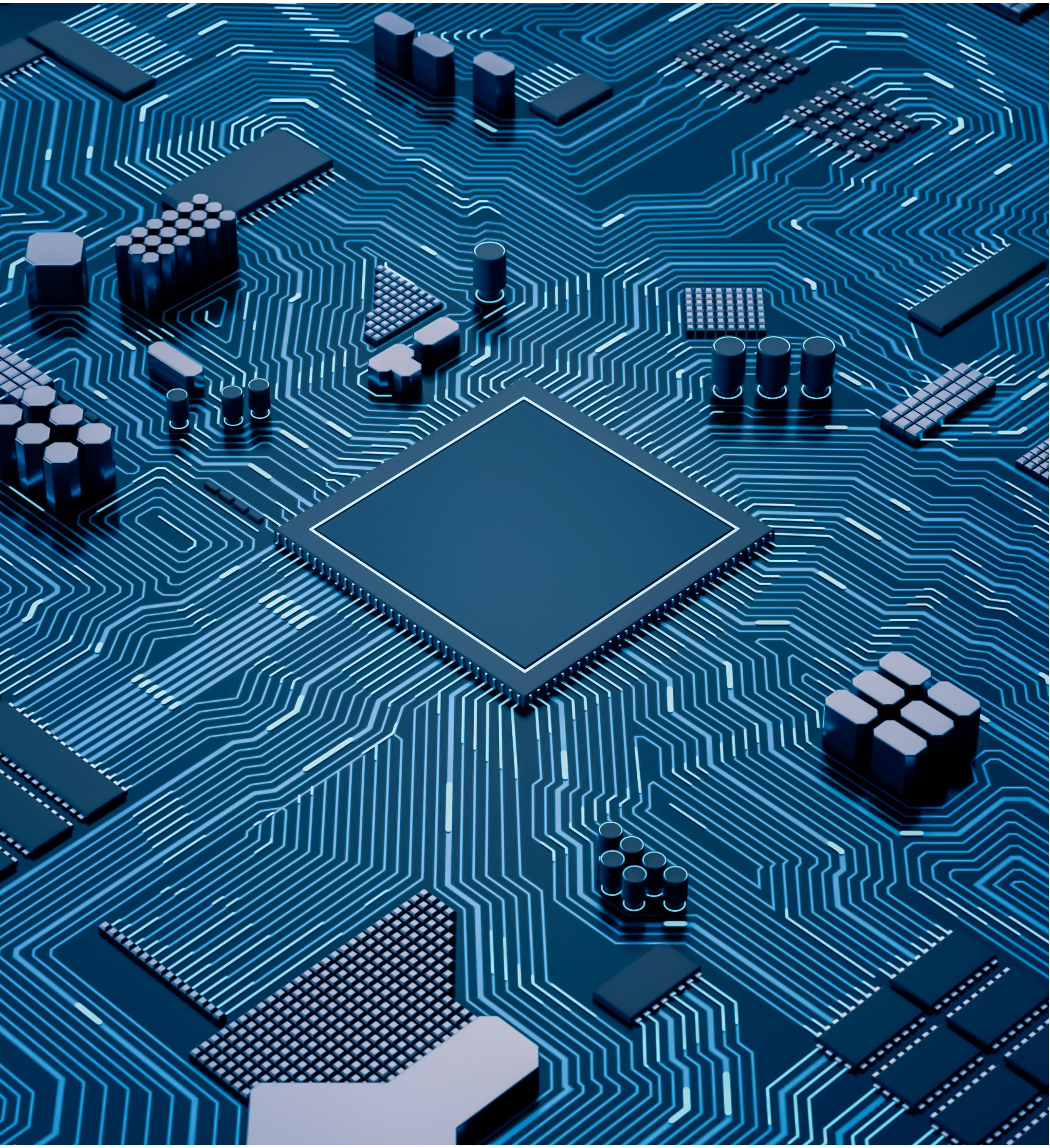
THE UNIVERSITY OF SYDNEY

Acceptable Use of ICT Resources Policy 2025



About this document

Printed or electronic copies may be out of date. Always check the Policy Register for the current version.

Title page image credit: Adobe Stock

Table of contents

Concept map 4

Part 1 Purpose and application 5

1.1 Purpose 5

1.2 Start date 5

1.3 Application 5

Part 2 Acceptable use 6

2.1 User responsibilities 6

Part 3 Unacceptable use 7

3.1 Content 7

3.2 Access 7

3.3 Technical restrictions 7

3.4 Emails and messages 8

Part 4 Special use 9

4.1 Use of prohibited and restricted material 9

4.2 Personal use 9

4.3 Personal devices 10

Part 5 Terms of use 11

5.1 Service 11

5.2 Loss or damage 11

5.3 Privacy 11

5.4 Our rights 11

Part 6 Cyber security events 13

6.1 Cyber security 13

Part 7 Misuse 14

7.1 Misuse outcomes 14

Part 8 Breaches of this Policy 15

Part 9 Roles and responsibilities 16

9.1 Users 16

9.2 Authorised University officer 16

9.3 Chief Information Officer 16

9.4 Heads of organisational units 16

9.5 Business owners 16

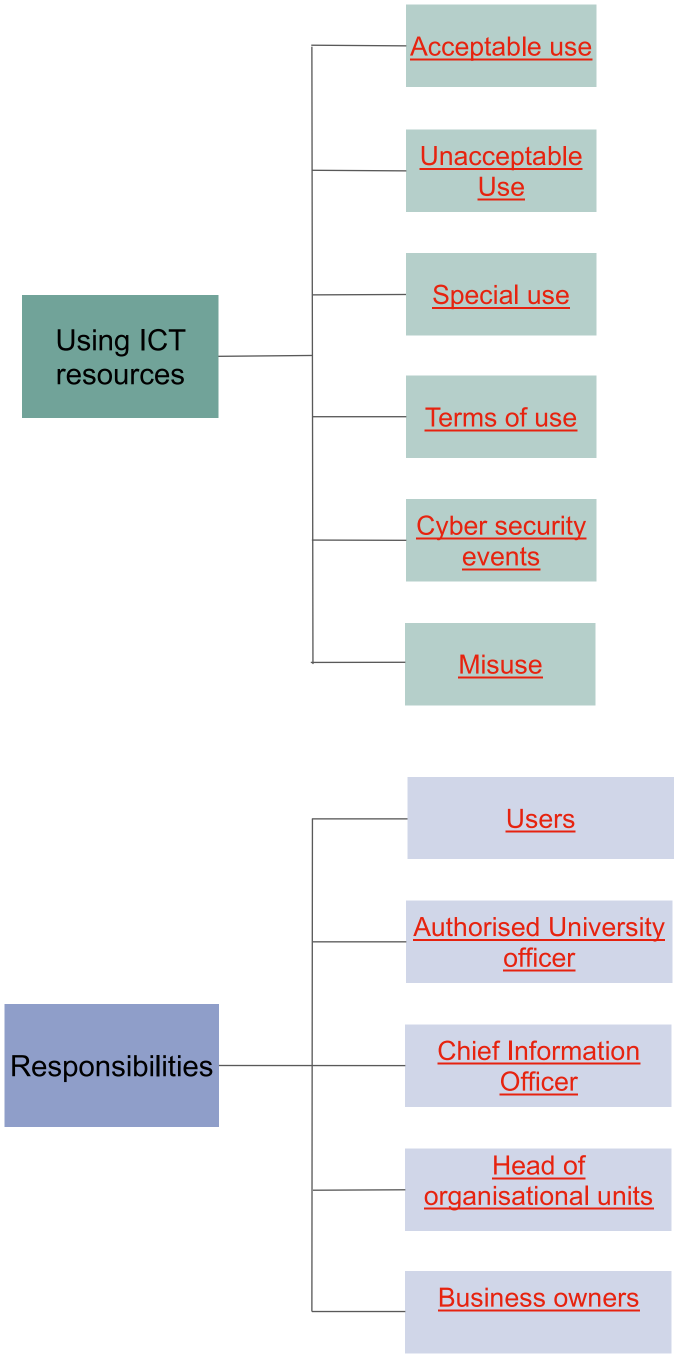
Part 10 Definitions 17

Part 11 Notes 24

Part 12 Amendment history 26

Concept map

The keywords in the concept map below are clickable. You can return to this concept map by pressing [Alt] + [←].



Part 1 Purpose and application

1.1 Purpose

(1) This Policy explains:

(a) the principles for using our ICT resources in a legal, ethical, and responsible manner;

(b) which uses of our ICT resources are acceptable;

(c) the conditions that limit acceptable use;

(d) which uses of our ICT resources are prohibited; and

(e) the consequences of misuse.

(2) This Policy establishes:

(a) compliance requirements for users of our ICT resources; and

(b) requirements for reporting cyber security events.

1.2 Start date

(1) This Policy commences on 2 June 2025.

1.3 Application

(1) This Policy applies to all users of our ICT resources.

(2) The obligations of staff and affiliates under this Policy are in addition to their obligations under:

(a) the *Staff and Affiliates Code of Conduct*;

(b) the *Public Comment and Social Media Policy*;

(c) the *Work Health and Safety Policy;* and

(d) the *Charter of Freedom of Speech and Academic Freedom*.

(3) The obligations of students under this Policy are in addition to their obligations under the *Student Charter*.

Part 2 Acceptable use

2.1 User responsibilities

(1) Users of our ICT resources must comply with applicable laws, University policies, University procedures, and Cyber Security Technical Standards.

Note: Any conduct which occurs using, or is facilitated by, University ICT resources or other University equipment is 'University-related conduct' for the purposes of University policies and procedures.

(2) When using ICT resources, users must uphold the University values of excellence, trust, and accountability.

(3) When using ICT resources all users must act in accordance with the University's ethical framework and the *Charter of Freedom of Speech and Academic Freedom*.

(4) Users are responsible for all activities that knowingly, recklessly or negligently originate from their University account.

(5) Users must take all reasonable steps to protect our ICT resources from physical theft, data theft, damage, or unauthorised use.

(6) Users must only store, process or transmit digital information which is not generally available to the public using our ICT resources.

Note: For example, a user would not be permitted to send University records or operational information using a non-University approved email account. See the *Cyber Security Technical Standards* for Data Classification and Handling for further information.

Part 3 Unacceptable use

3.1 Content

(1) A user must not:

(a) bully, harass, sexually harass, abuse or intimidate any other person;

Note: For further information see the *Bullying, Harassment and Discrimination Prevention Policy*.

(b) unlawfully discriminate against any other person;

Note: For further information see the *Bullying, Harassment and Discrimination Prevention Policy* and the *Anti-Discrimination Act 1977 (NSW)*.

(c) access, store or transmit prohibited or restricted material, except as explained in clause 4.1;

(d) collect, use or disclose personal information, except as allowed by the *Privacy Policy* and the *Privacy Procedures*;

(e) breach copyright, or software or digital content licence conditions.

Note: See the *Intellectual Property Policy*.

3.2 Access

(1) A user must not:

(a) use another person's University account;

(b) facilitate or permit the use of our ICT resources by anyone not authorised by us;

(c) attempt to gain unauthorised access to any of our ICT resources;

(d) gain unauthorised access to external services;

(e) use our ICT resources in ways that are likely to corrupt, damage or destroy our data, software or hardware;

(f) use our ICT resources in ways that are likely to corrupt, damage or destroy any other person's data, software or hardware; or

(g) use our ICT resources to represent, or create the impression that they represent, the University unless expressly authorised to do so.

3.3 Technical restrictions

(1) A user must not:

(a) test, bypass, deactivate or modify the function of any cyber security control;

(b) knowingly install or use malware; or

(c) knowingly, recklessly or negligently connect compromised devices to our assets.

(2) The restrictions in clause 3.3(1) do not apply when the action:

(a) is for research or teaching purposes;

(b) is in an isolated testing environment; and

(c) has the explicit written approval of an authorised University officer.

(i) Authorised University officers must notify the Cyber Security Operations Team of all approvals they give.

3.4 Emails and messages

(1) A user must not send:

(a) junk mail;

(b) for-profit messages; or

(c) chain mail.

(2) A user must not send commercial email (including marketing or promotional emails) on behalf of the University unless:

(a) all intended recipients have consented, or the message is required by law;

(b) the University is clearly identified; and

(c) there is a clear option for the recipient to opt out of further emails of the same kind.

(i) Opt out mechanisms should be accessible for users with disabilities.

Note: Automated unsubscribe processes do not always work with accessibility software. In such cases an accessible alternative, such as an email option to request to be unsubscribed, should be included. Further information is available from the *Accessibility intranet page*.

(3) A user must not send commercial emails on behalf of a third party unless:

(a) all intended recipients have clearly consented;

(b) both the University and the third party are clearly identified; and

(c) there is a clear option for the recipient to opt out of further emails of the same kind.

(4) Bulk emails and messages should only be sent in accordance with the *Email and Electronic Messaging Policy*.

Note: See also the *Spam Act 2003 (Cth)*.

Part 4 Special use

4.1 Use of prohibited and restricted material

(1) Users must not access, store, or transmit prohibited material on, or using, our ICT resources, unless the use:

(a) is for research or teaching purposes;

(b) is consistent with any applicable Human Ethics Committee approval;

(c) is in accordance with all laws, policies, procedures, and *Cyber Security Technical Standards*; and

(d) is approved in writing by an authorised University officer.

(i) Authorised University officers must notify the Cyber Security Operations Team of all approvals they give.

(2) Users must not access, store, or transmit restricted material on, or using, our ICT resources, unless the use:

(a) is consistent with the requirements of clause 4.1(1); or

(b) is on a personal device:

(i) within a University-owned or affiliated student accommodation that permits that use; and

(ii) uses the residential wired network ports or University-provided residential Wi-Fi network.

4.2 Personal use

(1) A user may make limited personal use of our ICT resources.

(2) Limited personal use:

(a) is of a purely personal nature;

(b) does not involve excessive use of ICT resources (including printing resources);

(c) does not impose an unreasonable burden on an ICT resource, or impose additional costs on the University;

(d) does not unreasonably deny any other user access to any ICT resource;

(e) does not interfere with the normal operation of the University's network or its electronic storage capacity;

(f) does not contravene any law, or University policy or procedure; and

(g) where a user is a member of staff or an affiliate, does not interfere with their duties or the conduct of the University's operations.

(3) Our ICT resources must not be leased, loaned, or made available to a third party.

(4) Users must not use our ICT resources for unauthorised financial or commercial purposes for themselves or any third party.

Note: See the *Staff and Affiliates Code of Conduct* and the *Outside Earnings of Academic Staff Policy*.

(5) Users must not use our ICT resources to generate or process crypto currency except:

(a) for research or teaching purposes; and

(b) with written approval of an authorised University officer.

Note: The use of a crypto-currency wallet for a payment is not considered processing for the purposes of this policy.

4.3 Personal devices

(1) A user may use a personal device to:

(a) connect to a University Wi-Fi network; or

(b) remotely access our ICT resources through the Internet.

(2) Personal devices may only be connected to the University's network in accordance with the *Cyber Security Technical Standards*.

(3) Except for users of disability assistive devices, personal devices must not be connected to a wired network port within the University without authorisation.

(a) Users of disability assistive devices:

(i) may connect such devices if they are necessary for their work or study; but

(ii) must consult the Cyber Security Team as soon as possible about the devices they wish to use.

Part 5 Terms of use

5.1 Service

(1) We do not guarantee that our ICT resources will:

(a) always be available; or

(b) be free from any defects, including malware.

5.2 Loss or damage

(1) We accept no responsibility for loss or damage, including consequential loss or damage, or loss of data, arising from:

(a) the use of our ICT resources; or

(b) the maintenance and protection of our ICT resources.

(2) We may take any necessary action to mitigate any threat to our ICT resources, with or without prior notice.

5.3 Privacy

(1) Use of our ICT resources is not considered private. Users do not have the same rights as they may have when using a personal device through commercial service providers.

(2) All electronic communications that use our ICT resources:

(a) may be recorded and monitored in accordance with the *Workplace Surveillance Act 2005 (NSW)* and the *Cyber Security Technical Standards*;

(b) remain in the custody and control of the University;

(c) are subject to the *Government Information (Public Access) Act 2009 (NSW)*; and

(d) may be subject to:

(i) the *Privacy and Personal Information Protection Act 1998 (NSW)*;

(ii) the *Health Records and Information Privacy Act 2002 (NSW)*;

(iii) and the *State Records Act 1998 (NSW)*.

5.4 Our rights

(1) We may at any time, in accordance with any applicable University policies and procedures, *Cyber Security Technical Standards*, and legal obligations:

(a) limit the use of our ICT resources, with or without notice;

(b) view and copy digital information stored, processed, or transmitted using our ICT resources; and

(c) monitor, inspect, access, or examine any University ICT resource for any lawful purpose.

(2) Personal use of our ICT resources may result in the University holding personal information about users or others.

(a) We may access and use that information to ensure compliance with this policy, other policies, and legal obligations.

(3) We may at any time require a user to:

(a) acknowledge in writing that they will comply with this policy; or

(b) complete relevant training in the University's policies and procedures.

Part 6 Cyber security events

6.1 Cyber security

(1) Any person who identifies or suspects a cyber security event, control deficiency, or vulnerability must report it as soon as possible to:

(a) our Shared Service Centre; or

(b) the ICT Cyber Security Operations Team.

Note: Physical security events, including theft of ICT assets and non-digital information, should be reported to Protective Services.

(2) Any person who identifies or suspects a data breach resulting from a cyber security event, must also report the breach to the Privacy Team under the *Data Breach Policy*.

Note: See also the *Reporting Wrongdoing Policy*.

(3) Except where required or authorised by law, University policy or procedures, or applicable *Cyber Security Technical Standards*, a user must not communicate to external parties our:

(a) cyber security risks;

(b) controls;

(c) events; or

(d) incidents.

Part 7 Misuse

7.1 Misuse outcomes

(1) The Chief Information Officer, or a person authorised by them to do so, may determine that misuse or suspected misuse of our ICT resources has occurred.

(2) Where misuse or suspected misuse has occurred, we may:

(a) withdraw or restrict a user's access to our ICT resources;

(b) for staff and affiliates, commence disciplinary action under the *Staff and Affiliates Code of Conduct* and the *Enterprise Agreement 2023–2026*;

(c) for students, commence action for misconduct under the *University of Sydney (Student Discipline) Rule*; and

(d) notify the NSW Police and other relevant government authorities.

Part 8 Breaches of this Policy

8.1 What is a breach

(1) A breach of this Policy may constitute:

(a) a breach of the:

(i) *Student Charter*;

(ii) *Staff and Affiliates Code of Conduct*;

(iii) *Bullying, Harassment and Discrimination Prevention Policy*;

(iv) *Work Health and Safety Policy*; or

(v) *Research Code of Conduct*.

(b) misconduct under the:

(i) *University of Sydney Enterprise Agreement 2023-2026*;

(ii) *University of Sydney (Student Discipline) Rule*.

(2) A person will have acted in breach of this Policy if they have:

(a) personally breached the Policy;

(b) materially assisted or encouraged another person to breach the Policy; or

(c) promoted conduct in breach of this Policy on social media or elsewhere.

Note: News reports or social media posts that refer to a breach having occurred without endorsing the unauthorised conduct will not breach this requirement.

8.2 Breach outcomes

(1) The consequences of a breach of this Policy will depend on its type and severity.

(2) Breaches may result in any of:

(a) access to ICT resources being limited or discontinued;

(b) disciplinary action by the University; and

(c) in the case of serious breaches, civil or criminal proceedings.

Part 9 Roles and responsibilities

9.1 Users

(1) comply with the requirements of this Policy.

9.2 Authorised University officer

(1) approves exceptions to technical restrictions (clause 3.4);

(2) approves the access, storage, or transmission of prohibited or restricted material on our ICT resources (clause 4.1);

(3) approves the generation or processing of cryptocurrency (clause 4.2(5)); and

(4) informs the Cyber Security Operations Team of all approvals given (clauses 3.3 and 4.1).

9.3 Chief Information Officer

(1) determines that misuse or suspected misuse of our ICT resources has occurred (clause 7(1)); and

(2) when appropriate, authorises another person to determine if misuse or suspected misuse of ICT resources has occurred (clause 7.1).

9.4 Heads of organisational units

(1) identify roles within their unit that may have privileged access to ICT resources; and

(2) require that they are controlled in accordance with any applicable *Cyber Security Technical Standards*.

9.5 Student representative organisations

(1) use University ICT resources consistently with their constitutions and this policy.

9.6 Business owners

(1) require all access to, and data within, ICT resources within their remit to be controlled in accordance with any applicable University Policy and Procedures, *Cyber Security Technical Standards* and legal obligations; and

(2) engage with ICT for any acquisition of technology or external ICT services in accordance with:

(a) the *Procurement Policy*;

(b) delegations of authority as set out in the *University of Sydney (Delegations of Authority) Rule 2020*; and

(c) any applicable *Cyber Security Technical Standards*.

Part 10 Definitions

(1) In this Policy a reference to ‘we’, ‘our’ or ‘us’ means the University.

authorised University officer

any of:

- Principal Officer;
- Executive Dean;
- Dean;
- Head of School and Dean of a University school;
- Head of Clinical School; and
- Head of School.

business owner

A senior staff member who is the specified owner of a business capability or technology offering. They are responsible for cyber security and risk in accordance with the *Cyber Security Policy*.

- Academic information systems and audio-visual technology services are examples of business capabilities.
- Research computing is an example of a technology offering.

commercial email

an email message offering, promoting or marketing a good or service.

control deficiency

weakness in an information system, internal controls, external controls, or implementation that could be exploited.

chain mail

a communication which includes a request that the recipient forward it to others to obtain a reward or avoid a negative consequence.

cyber security

as set out in the *Cyber Security Policy*.

> the measures we take to:
>
> - protect ICT, digital information systems, networks, devices and digital information from compromise or interruption; and
> - facilitate rapid and effective detection and response to any compromise or interruption of an ICT resource.

cyber security control

as set out in the *Cyber Security Policy*.

> any management, operational or technical measure (including safeguards or countermeasures) put in place for cyber security.

cyber security event

as set out in the *Cyber Security Policy*.

an event relating to any cyber security control protecting our ICT resources from compromise or interruption. This includes internal or external acts which:

- may bypass or contravene applicable controls, policies or procedures; or
- may potentially compromise the confidentiality, integrity or availability of ICT resources.

Cyber Security Technical Standards

define the specific mandatory requirements determined by the Chief Information Officer under clauses 2.3 and 3.7 of the *Cyber Security Policy*.

digital information

information that is in a digital or electronic form; and is stored, processed, or transmitted within an ICT service or an ICT asset.

electronic communication

is a message sent using:

- ICT resources; or
- any communication, collaboration, or carriage service the University provides; and
- to an electronic address in connection with:
  - an email account; or
  - an instant messaging account; or
  - a telephone account; or
  - a similar account.

Note: Email addresses and telephone numbers are examples of electronic addresses.

ethical framework

the expectations and requirements established through the operation and interaction of:

- the *Staff and Affiliates Code of Conduct*;
- the *Student Charter*;
- the *Research Code of Conduct*;
- the *Business Ethics Statement* ;
- the *Academic Integrity Policy*; and
- the *Higher Degree by Research Supervision Policy*

excessive use

personal use of ICT resources that consumes significant ICT resources or interferes with a user’s role and responsibilities or academic performance.

hardware

the physical components of a device or electronic system, such as:

- desktops
- laptops
- mobile phones
- network hubs
- audio-visual equipment
- instrumentation
- virtualised hardware.

Hardware also includes peripheral devices like:

- printers
- monitors
- webcams
- keyboards
- mice
- speakers
- microphones
- portable storage devices.

ICT

Information and Communications Technology

ICT asset

any hardware, software, cloud-based services, communication devices, data centres or networks that are owned by the University or provided by the University to users.

ICT resource

any ICT service, ICT asset or digital information.

ICT service

any business or technology function that we provide using one or more ICT assets. This includes:

- application systems (including software-as-a-service); and
- ICT infrastructure services; such as operating systems, databases, voice and data telecommunications services, network services, media services, file and print services, and email services.

junk mail

unsolicited advertising or promotional material

limited personal use

use that is consistent with the requirements of clause 4.2.

malware

hardware, firmware, software or any type of code that is intended to perform an unauthorised process that may have an adverse impact on an ICT resource or person.

misuse

use of the University's ICT resources in contravention of any law or University policy, procedures or relevant *Cyber Security Technical Standards*.

organisational unit

any of:

- a faculty;
- a University school;
- a portfolio or professional services unit controlled by a Principal Officer; and
- a Level 4 Centre as described in the *Centres Policy*.

personal device

a non-University-owned or provided device that is used by an individual to access, store, process or transmit University data or digital information. This includes:

- desktop and laptop computers;
- personal digital assistants;
- tablets;
- smartphones;
- mobile PIN pads;
- radio communication devices;
- USB keys; and
- any form of portable data storage device.

Principal Officer

as set out in the *University of Sydney (Delegations of Authority) Rule*.

means any of:

- Vice-Chancellor and President;
- Provost and Deputy Vice-Chancellor;
- Deputy Vice-Chancellor;
- Vice-President;
- General Counsel;

privileged access

special or elevated access or abilities beyond those of a standard user.

prohibited material

illegal and restricted content, such as:

- child exploitation material, including child pornography or material that instructs on, promotes or incites child abuse;
- content that shows extreme sexual violence or materials that are overly violent;
- materials that provoke the viewer into committing crimes and carrying out violent acts, such as material that instructs on, promotes or incites violent acts;
- material that vilifies a person or group of people, or instructs on, promotes, or incites discrimination; and
- content that promotes terrorism or encourages terrorist acts.

Residential College

any of:

- Mandelbaum House;
- Sancta Sophia College;
- St Andrew’s College;
- St John’s College;
- St Paul’s College;
- Wesley College;
- Women’s College.

restricted material

content that:

- is obscene or pornographic material permitted by law; or
- is material that instructs or promotes gambling.

student representative organisation

as set out at clause 7.1 of the *Student Associations Policy*. That is any of:

- Sydney University Postgraduate Representative Association (SUPRA);
- Sydney University Sport and Fitness Limited (SUSF);
- University of Sydney Students' Representative Council (SRC);
- University of Sydney Union (USU.)

University account

the access to University ICT resources that we provide to a holder of a Unikey or University email address.

University-related conduct

any conduct that is connected to the University, including conduct that:

- refers or relates to the University, its activities, or its staff, affiliates or students in their status as staff, affiliates or students of the University;
- occurs on, or in connection with, University lands or other property owned by the University;
- occurs at, or in connection with, a Residential College;
- occurs at or in connection with University owned or affiliated student accommodation;
- occurs using, or is facilitated by, University ICT resources or other University equipment;
- occurs during, or relates to, the performance of duties for the University;
- occurs during, or in connection to, any University-related function or event (whether sanctioned or organised by the University or not) or when representing the University in any capacity;
- occurs during, or in connection to, any event run by or affiliated with student representative organisations, student clubs or student societies (whether sanctioned or organised by the University or not);
- occurs during, or in connection to, students’ clinical, practicum, internship or work experience placements; or
- occurs while a University of Sydney student is participating in an overseas exchange, study abroad or other approved program.

University values

the values that serve as guiding principles for behaviour and decision-making at the University. They are:

- Excellence – pursuing outstanding performance in service to our communities
- Trust – actively creating an inclusive and collaborative work environment
- Accountability – owning our successes and failures, both collectively and individually

user

a person or entity that uses the University's ICT resources.

vulnerability

a weakness in the design, implementation or operation of an ICT Resource, system component or security control, that could be exploited or triggered by a threat.

Part 11 Notes

Recissions and replacements

This document replaces the following, which are rescinded as from the date of commencement of this document:

(1) *Acceptable Use of ICT Resources Policy 2019*, which commenced on 1 August 2019

Acceptable Use of ICT Resources Policy 2025

Date approved	26 May 2025
Date commenced	2 June 2025
Date for review	2 June 2030
Approver	Vice-President (Operations)
Owner(s)	Chief Information Officer
Date last amended	
Related documents	*Spam Act 2003 (Cth)* *Anti-Discrimination Act 1977 (NSW)* *Government Information (Public Access) Act 2009 (NSW)* *Health Records and Information Privacy Act 2002 (NSW)* *Privacy and Personal Information Protection Act 1998 (NSW)* *State Records Act 1998 (NSW)* *Workplace Surveillance Act 2005 (NSW)* *University of Sydney (Delegations of Authority) Rule* *University of Sydney (Student Discipline) Rule* *Charter of Freedom of Speech and Academic Freedom* *Student Charter* *Staff and Affiliates Code of Conduct* *Bullying, Harassment and Discrimination Prevention Policy* *Cyber Security Policy* *Email and Electronic Messaging Policy* *Intellectual Property Policy* *Outside Earnings of Academic Staff Policy* *Privacy Policy*

Public Comment and Social Media Policy

Privacy Procedures

Data Breach Policy 2023

Recordingkeeping Policy

Work Health and Safety Policy

Working with Children and Vulnerable Adults Policy

Reporting Wrongdoing Policy

Enterprise Agreement 2023–2026

Viva Engage Terms of Use

Part 12 Amendment history

Register Version	Approved by	Clause	Amendment	Commenced