ACCEPTABLE USE OF ICT RESOURCES POLICY 2019

The Vice-Chancellor as delegate of the Senate of the University of Sydney, as the governing authority of the University of Sydney, by resolution adopts the following policy.

Dated: 15 July 2019

Last amended: 18 February 2021 (administrative amendments)

Signature:

Position: Vice Chancellor

CONTENTS

1 Name of policy

This is the Acceptable Use of ICT Resources Policy 2019.

2 Commencement

This policy commences on 1 August 2019.

3 Policy is binding

Except to the extent that a contrary intention is expressed, this policy binds the University, staff, students and affiliates.

4 Statement of intent

This policy:

(a) sets out the principles for ensuring the University's ICT resources are used in a legal, ethical and responsible manner;

(b) sets out the conditions of personal use of the University's ICT resources;

(c) informs users of University ICT resources of their responsibilities and the penalties for misuse;

(d) establishes compliance requirements for users of the University's ICT resources;

(e) establishes requirements for reporting cyber security events; and

(f) reflects the University's values of:

(i) respect and integrity; and

(ii) openness and engagement;

Note: See the *University's Strategic Plan 2016-20*.

5 Application

(1) This policy applies to all users of the University's ICT resources.

(2) For the avoidance of doubt:

(a) the obligations of staff and affiliates under this policy are in addition to obligations set out in the *Code of Conduct – Staff and Affiliates*, the *Public Comment Policy* and the *Charter of Freedom of Speech and Academic Freedom*.

(b) the obligations of students under this policy are in addition to obligations set out in the *Code of Conduct for Students*.

6 Definitions

In this policy:

authorised University officer	means any of: • Principal Officer; • Executive Dean; • Dean; • Head of School and Dean of a University school; • Head of Clinical School; • Head of School.

cyber security	has the meaning provided in the *Cyber Security Policy 2019*, which at the date of this policy is: the measures taken to: • protect information and communications technology, electronic systems, networks, devices and digital information from compromise or interruption; and • facilitate rapid and effective detection and response to any compromise or interruption.
cyber security control	means any management, operational or technical measure (including safeguards or countermeasures) put in place for cyber security.
cyber security event	has the meaning given in the *Cyber Security Policy 2019* which at the date of this policy is: means an event relating to any cyber security control protecting University 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.
digital information	means information that is in a digital or electronic form and is stored, processed or transmitted within an ICT service or an ICT asset
Head of Administrative Area	has the meaning given in the *University of Sydney (Delegations of Authority) Rule 2016*. At the date of this policy this is: a senior staff member, outside a faculty or University school, whose position is declared as such by the Vice-Chancellor in writing and recorded as such in the relevant human resources recordkeeping systems.
ICT	means information and communications technology within the remit of any University organisational unit.
ICT asset	means 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	means any ICT service, ICT asset or digital information.
ICT service	means any business or technology function provided using one or more ICT assets including but not limited to: • 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.

limited personal use	means use that is consistent with the requirements of clause 10.
misuse	means use of the University's ICT resources in contravention of any law or University policy, procedures or relevant technical standards.
organisational unit	means any of the following: • faculty; • University school; • a portfolio or professional services unit controlled by a Principal Officer; • a level 4 centre, as described in the *Centres and Collaborative Networks Policy 2017*.
personal device	means 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 desktops and laptop computers, personal digital assistants, tablets, smartphones, mobile PIN pads, radio communication devices, USB keys or any form of portable storage device.
Principal Officer	has the meaning given in the *University of Sydney (Delegations of Authority) Rule 2016*. At the date of these procedures, this is: a collective reference, for the purpose of this document to: Vice Chancellor and Principal Deputy Vice-Chancellor Vice Principal General Counsel Director, University Libraries
prohibited material	means illegal content, such as: • child exploitation material including child pornography or material that instructs, 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. This might be material that instructs, promotes or incites violent acts; • material that is vilificatory or instructs, promotes or incites discrimination; and • content that promotes terrorism or encourages terrorist acts.
restricted material	means content that: • is obscene or pornographic material permitted by law; or • is material that instructs or promotes gambling.

technical standards	means the mandatory standards for specific ICT activities determined by the Chief Information Officer under clauses 8 and 10 of the *Cyber Security Policy 2019*
University account	means the access to University ICT resources provided to holders of a Unikey or University email address.

7 Compliance

(1) Users of the University's ICT resources must comply with applicable:

(a) laws;

(b) University policies;

(c) University procedures; and

(d) the technical standards.

(2) Users must not use University ICT resources to:

(a) harass, menace, defame, vilify or discriminate against any other person;

Note: Refer to the *Bullying, Harassment and Discrimination Prevention Policy 2015*.

(b) collect, use or disclose personal information except in accordance with the *Privacy Policy 2017* and *Privacy Procedures 2018;*

(c) infringe copyright or breach University software licence restrictions.

Note: Refer to the *Intellectual Property Policy 2016*.

(d) distribute:

(i) junk mail;

(ii) for-profit messages;

(iii) chain mail; or

(iv) unsolicited commercial emails; including

(v) commercial emails on behalf of the University (including marketing and promotional emails), unless all intended recipients have consented or the message is required by law, the University is clearly identified and there is a clear means for the intended recipient to opt out of further commercial emails of the same kind; and

(vi) commercial emails on behalf of a third party, unless all intended recipients have clearly consented, both the University and the third party are clearly identified, and there is a clear means for the intended recipient to opt out of further commercial emails of the same kind.

Note: Refer to the *Spam Act 2003 (Cth).*

8 Restricted and Prohibited Use

(1) Users must not access, store or transmit prohibited material on the University's ICT resources except:

(a) for research or teaching purposes;

(b) in accordance with all laws, policies, procedures and technical standards; and

(c) with express written approval of an authorised University officer.

(2) Users may only use the University's ICT resources to access restricted material:

(a) using a personal device;

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

(ii) using the residential wired network ports or University provided residential WiFi network;

(b) or for research or teaching purposes;

(i) consistent with the requirements of subclause 8(1); and

(ii) with express written approval of an authorised University officer.

9 User responsibilities

(1) Users are responsible for all activities originating from their University account.

(2) Users must take all reasonable steps to protect the University's ICT resources from physical theft, damage or unauthorised use.

(3) Users must not:

(a) use another person's account;

(b) facilitate or permit the use of the University's ICT resources by anyone not authorised by the University;

(c) attempt to gain unauthorised access to any university ICT resource;

(d) gain unauthorised access to external services;

(e) use University ICT resources in ways which are likely to corrupt, damage or destroy the University's or any other person's data, software or hardware.

(4) Users must not

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

(b) knowingly install or use malicious software;

(c) connect compromised devices to University assets

except

(d) for research or teaching purposes;

(e) with express written approval from an authorised University officer; and;

(f) in an isolated testing environment;

(5) Users must only store, process or transmit the University's highly protected digital information using:

(a) University approved systems; or

(b) personal devices, that are:

(i) encrypted using University approved mechanisms; and

(ii) protected using a strong password, PIN or equivalent control.

Note: See the *Cyber Security Policy 2019* ; *Cyber Security Standard – Data Classification*, *Cyber Security Standard – Data Handling*

(6) Users are responsible for determining the controls to apply when storing, processing or transmitting their own personal information using the University's ICT resources for personal use.

10 Personal use of University ICT Resources

(1) Users are permitted personal use of the University's ICT resources, of a limited nature.

(2) Limited personal use:

(a) is of a purely personal nature;

(b) does not directly or indirectly impose an unreasonable burden on any ICT resource, or burden the University with incremental costs;

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

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

(e) in the case of staff and affiliates, does not interfere with the execution of duties.

(3) Users must not use the University's ICT resources to generate or process crypto-currency except:

(a) for research or teaching purposes; and

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

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

(4) The University's ICT resources must not be leased, lent or otherwise made available to third parties for personal profit.

(5) Staff and affiliates must not use University ICT resources for financial or commercial gain for themselves or any third party.

Note: Staff and affiliates should refer to the *Code of Conduct – Staff and Affiliates.* Academic staff should also refer to the *Outside Earnings of Academic Staff Policy 2011.*

11 Personal devices

(1) Users may use a personal device to:

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

(b) remotely access ICT resources through the Internet.

(2) Users must not connect a personal device to a wired network port within the University:

(a) without authorisation; or

(b) with a known security vulnerability.

(3) Users must only connect a personal device to the University's network in accordance with the technical standards.

12 Terms of Use and Limitations on Use

(1) The University does not guarantee that University ICT resources will:

(a) always be available; or

(b) be free from any defects, including malicious software.

(2) The University accepts no responsibility for loss or damage (including consequential loss or damage or loss of data) arising from:

(a) the use of University ICT resources; or

(b) the maintenance and protection of ICT resources.

(3) The University may take any necessary action in accordance with the technical standards, in order to mitigate any threat to the University's ICT resources, with or without prior notice.

(4) The use of University ICT resources is not considered private. All electronic communications using University ICT resources:

(a) may be recorded and monitored in accordance with the technical standards;

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

(c) may be subject to the

(i) *Privacy and Personal Information Protection Act 1997*;

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

(iii) *State Records Act 1998 (NSW);*

(d) remain in the custody and control of the University.

Note: Users of ICT Resources should be aware that they do not have the same rights as they would using personally owned devices through commercial service providers.

(5) The University reserves the right to:

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

(b) view and copy digital information stored, processed or transmitted using the University's ICT resources; or

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

in accordance with the technical standards.

Note: Users should be aware that personal use of the University's ICT Resources may result in the University holding personal information about the user or others which may then be accessed and used by the University to ensure compliance with this, and other policies.

(6) The University may at any time require a user to:

(a) acknowledge in writing that they will abide by this policy; or

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

13 Cyber security events

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

(a) the University's Shared Service Centre; or

(b) ICT unit Cyber Security Team.

14 Misuse

(1) In the event of misuse or suspected misuse of the University's ICT resources (as determined by the Head of Cyber Security), the University may:

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

(b) commence disciplinary action;

(i) for staff or affiliates: disciplinary action in accordance with the *Code of Conduct Staff and Affiliates* and the *University of Sydney Enterprise Agreement 2018-2021;*

(ii) for students: action for misconduct under the *Code of Conduct for Students* and the *University of Sydney (Student Discipline) Rule 2016;* and

(c) notify the Police or other relevant government authority.

15 Rescissions and replacements

This document replaces the *Policy on the Use of Information and Communications Technology Resources,* which is rescinded as from the date of commencement of this policy.

NOTES

Acceptable Use of ICT Resources Policy 2019

Date adopted:	15 July 2019
Date commenced:	1 August 2019
Date amended:	18 February 2021
Administrator:	Chief Information Officer
Review date:	1 August 2024
Rescinded documents:	*Policy on the Use of Information and Communication Technology Resources.*
Related documents:	*Copyright Act 1968 (Cth)*
	Spam Act 2003 (Cth)
	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)
	University of Sydney (Delegations of Authority) Rule 2020
	University of Sydney (Student Discipline) Rule 2016
	Charter of Freedom of Speech and Academic Freedom
	Bullying, Harassment and Discrimination Prevention Policy 2015
	Code of Conduct – Staff and Affiliates
	Code of Conduct for Students
	Cyber Security Policy 2019
	Intellectual Property Policy 2016
	Outside Earnings of Academic Staff Policy 2011
	Privacy Policy 2017
	Cyber Security Procedures 2019
	Privacy Procedures 2018
	Public Comment Policy
	Recordkeeping Policy 2017
	University of Sydney Enterprise Agreement 2018 - 2012
	Payment Card Industry Data Security Policy 2019

AMENDMENT HISTORY

Provision	Amendment	Commencing
5(2)(a); Related documents	Reference to the Charter of Freedom of Speech and Academic Freedom added to subclause.	18 February 2021
Definitions; Related documents	Updated definition of Head of Administrative Area and definition of Principal Officer to reference University of Sydney (Delegations of Authority) Rule 2020.	18 February 2021