Acceptable use of ICT Resources Policy

1 Purpose

To outline the acceptable use of University Information and Communication Technology Resources (hereafter referred to as ICT Resources) by all Users.

This Policy will be reviewed on an annual basis and evaluated in line with changes to business processes and planning requirements.

2 Scope

This Policy applies equally to all Users of University ICT Resources.

3 Policy Statement

The University has identified the pivotal role of Information and Communication Technology (ICT) to enhance the academic program, research initiatives and support services available to Users.

This Policy sets out the University's stance on the acceptable use of ICT Resources in respect to the provision of these resources, access to resources, responsible ethical and legal use of resources, security and privacy, compliance, penalties and discipline.

This Policy aligns with:

- *Higher Education Standards Framework (Threshold Standards) 2021*: Standard 2.1 Facilities and Infrastructure

4 Principles

The University will ensure that appropriate management controls are implemented in relation to the acceptable use of ICT Resources. These will include:

4.1 Provision of ICT Resources

The University recognises the importance of ICT Resources and provides access to Users for the purpose of conducting University business and other authorised purposes according to need and Availability of resources. Usage is subject to the terms and conditions set out in this Policy and associated procedures.

The University does not permit its ICT Resources to be used for unauthorised activities. Should any User become aware of any action by another individual which could be considered to breach this Policy, they are requested to take appropriate action to ensure it is brought to the attention of ICT management.

The University accepts no responsibility for loss or damage, consequential loss or damage, or loss of data arising from the use of its ICT Resources or the maintenance of its ICT Resources.

4.2 Privacy

Users who have authorised access to private information about Employees or Students, or confidential information of the University must respect the privacy of others and maintain the Confidentiality of the information to which they have access in accordance with privacy laws and any University Policies.

Users should exercise caution when storing any confidential information in electronic format as the privacy of such information cannot be guaranteed.

4.3 Monitoring

Whilst the University respects the privacy of Users of ICT Resources, the University reserves the right to monitor User activity and take appropriate action if misuse of resources is identified.

Monitoring for misuse of University ICT Resources must be authorised by the Chief Information Officer. The University reserves the right to inspect all University owned ICT devices, together with all files, Employee email accounts and message, and logs contained on those devices. Awareness of these provisions shall be included as a mandatory component of all new Employee inductions.

The University reserves the right to examine files and directories where it is necessary to determine the ownership or recipient of lost or misdirected files, and also where the University has information or evidence that:

- System Integrity is threatened
- Security is compromised
- An activity has a detrimental impact on the quality of service to other Users
- The system is being used for purposes which are prohibited under this Policy
- The system is being used for unlawful purposes.

By connecting a privately owned ICT device (including wireless or remote connection) to the University network, any User acknowledges that:

- they will be bound by, and comply with, the terms and conditions of use of the University ICT Resources, as established in this Policy and the ICT Information Management and Security Policy

- the network traffic generated by a privately owned ICT device is generated in pursuit of University business only and that - while the traffic is traversing University networks - it is subject to the same right of inspection as traffic originating from University owned ICT devices.

ICT Services routinely monitor traffic on networks. Logs obtained from monitoring operations are used for capacity planning, performance measurement, security, accountability, and evidentiary purposes.

4.4 Software

The University requires that Users use and install software in compliance of the respective licence terms and conditions.

Making an infringing copy of software by an individual if the individual knows or ought reasonably to know that the copy is infringing copyright is a criminal offence.

Installation of privately purchased and owned software on University ICT Resources is not recommended. In all cases, ICT Employees will request proof of purchase (consisting of the licence certificate and original media, or invoice) before any software will be installed on a University ICT Resource.

4.5 Computing resources of students

The University provides on-campus computer facilities in line with equity principles and legislative requirements.

4.6 Information management and security

Users must take appropriate measures to ensure the Availability, Confidentiality, and Integrity of all University related information stored or received, including measures to prevent loss of information. Stakeholders should refer to the Information Management and Security Policy.

4.7 Records management

Users should also be aware that email communications are considered documents (records) of the University for the purposes of the *Public Records Act 2002,* the *Right to Information Act 2009* and the *Information Privacy Act 2009*.

4.8 Access

Access to Information through ICT Resources will only be provided if there is a legitimate requirement.

Users of University ICT Resources must protect:

- their online identity from use by another individual
- the Integrity of computer-based ICT Resources
- the privacy of electronic information.

Users must refrain from seeking to gain unauthorised access to ICT Resources or enabling unauthorised access. Any attempt to gain unauthorised access to a system or to another person's information is a violation of University Policy and may also violate applicable law which may result in either civil and/or criminal proceedings. However, authorised ICT Service system administrators may access ICT Resources, but only for a legitimate operational purpose and only the minimum access required to accomplish this legitimate operational purpose. Users are required to use Multi-Factor Authentication (MFA) to ensure an additional layer of security when accessing ICT resources.

- Sharing an online identity (user ID and /or password is prohibited).
- Users must not intentionally seek, access or provide information or passwords or other digital materials belonging to other Users, without the specific permission of those other Users.
- Users of University ICT Resources must not access computers, computer software, computer data or information, or computer networks without proper authorisation, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the University.

4.9 Access by minors

The University will take reasonable steps to ensure that restricted content is not accessible to minors (those under 18 years of age) without documented parental approval.

4.10 Acceptable use

The University's ICT environment is dynamic, characterised by openness, creativity and free sharing of information, to the greater benefit of universities generally. This Policy will respect this environment and inhibit these characteristics only when necessary to protect the essential

interests of the University.

- Limited Personal Use - It is acknowledged that reasonable limited personal use will occur. 'Limited personal use' means private use that is infrequent, brief and kept to a minimum. University ICT Resources should not be used for activities unrelated to appropriate University functions. The University accepts no liability for any loss or damages suffered by Users as a result of personal use.

- Illicit Material - Users must not send, view, download or store illicit, fraudulent, obscene or pornographic material that are a violation of applicable law or University Policy.

- Defamation, Harassment and Other Abusive Behaviour - No User will, under any circumstances take any action which would or might lead to the University's ICT Resources being used for the purpose of defaming or slandering any individual or organisation or use an ICT system in any way such that a reasonable individual may consider this action to be viewed as harassing, abusive or obscene behaviour.

- Copyright, Licences and Related Obligations - Users must not violate copyright law and must respect licences to copyrighted materials. Users must ensure confidentiality and re-use obligations are observed.

- Social Media - Users must respect the purpose of and abide by the terms and conditions of use of online forums, including social media networking websites, mailing lists, chat rooms, wikis and blogs.

- Commercial Use - University ICT Resources should not be used for commercial purposes, including advertisements, solicitations, promotions or other commercial messages, except as permitted under University Policy.

- Family and Domestic Violence - Users must not use University property or resources to engage in any actions resulting in Family and Domestic Violence.

4.11 Indemnity

The University is not responsible for the content of any material prepared, received, or transmitted by Users. As a condition of using the University's ICT Resources, Users will not violate any Commonwealth or State civil or criminal laws, and Users will comply with all Commonwealth, State and international copyright and other intellectual property laws and agreements and other Commonwealth and State laws. Furthermore, Users agree to indemnify, exonerate and protect the University (and its representatives) from any claim, damage, or cost related to the Users use of the University's ICT Resources.

4.12 Online content regulation compliance

Pursuant to the requirements of the *Broadcasting Services Act 1999*, the University endorses

and will support effective, practical and appropriate measures that assist the University and clients manage internet use.

4.13 Content takedown notice

The University will have in place a procedure for receiving and responding to takedown notices (as defined in the Act) issued by the Government Authority or third party organization within the timeframe required under the Act.

4.14 Identity management

The University Identity Management System (IDM) is responsible for the overall management and security of Employees, Student and pseudo accounts. Academic and administrative Employees will be authorised to access resources required to perform their duties. Students will be authorised to access services for academic purposes relating to their program of study at the University for the period of their enrolment. Users who are not Employees or Students may have pseudo or affiliate account access provided.

4.15 Compliance, breaches and disciplinary action

Users who become aware of a possible breach of this Policy must report it to:

- their Supervisor
- their organisational unit head
- the Chief Information Officer through the ICT Service Desk.

The Chief Information Officer is responsible in the first instance for handling and investigating potential breaches. Penalties and discipline are outlined in the ICT Information Management and Security Policy.

The University has obligations relating to copyright, intellectual property, privacy, right to information, sexual harassment, and racial discrimination as defined by law, and in its own policies. The University expects that Users of its ICT Resources will also exercise their responsibilities in this area. Users should familiarise themselves with University policies and documentation on the following matters:

- Code of Conduct Policy
- Intellectual Property Policy and subordinate Procedures
- Copyright

- Employee Diversity and Inclusion Policy.

The University has certain contractual obligations relating to the use of its ICT Resources which constrain the way facilities may be used. The University may take disciplinary action against anyone whose use of facilities violates the terms of such agreements. In addition to observing Australian laws, related University Policies and procedures, and this Policy, Users should familiarise themselves with any published acceptable use Policy associated with each service.

5 References

Universities and Colleges Information Systems Association (UCISA) *Information Security Management Toolkit Edition 1.0 Volume 1* Retrieved 17 March 2015, from https://www.ucisa.ac.uk/Resources/ISMT

6 Schedules

This policy must be read in conjunction with its subordinate schedules as provided in the table below.

7 Policy Information

Accountable Officer	Deputy Vice-Chancellor (Enterprise Services)
Responsible Officer	Deputy Vice-Chancellor (Enterprise Services)
Policy Type	Executive Policy
Policy Suite	Electronic Mail Distribution List and Group Schedule Information Systems Financial Management Procedure Use of Electronic Mail Procedure
Subordinate Schedules	
Approved Date	8/8/2024
Effective Date	8/8/2024
Review Date	14/12/2028
Relevant Legislation	*Broadcasting Services Act ALRC* *Copyright Act 1968 (Cth)*

	Crimes Act 1914 (Cth) *Criminal Code Act 1899 (Qld)* *Criminal Justice Act 1988 (Qld)* *Cybercrime Act 2001 (Cth)* *Electronic Transactions Act 2001 (Qld)* *Financial Accountability Act 2009 (Qld)* *Information Privacy Act 2009 (Qld)* *Public Records Act 2002 (Qld)* *Public Sector Ethics Act 1994 (Qld)* *Queensland Government Online standards, policies and legislation:* • Information security policy (IS18:2018) • Use of ICT services, facilities and devices policy (IS38) • Records Governance Policy *Right to Information Act 2009 (Qld)* *Spam Act 2003 (Cth)* *Telecommunications Act 1997 (Cth)* *Work Health and Safety Act 2011*
Policy Exceptions	Policy Exceptions Register
Related Policies	Academic Freedom and Freedom of Speech Policy Business Continuity Policy Code of Conduct Policy Employee Diversity and Inclusion Policy Enterprise Risk Management Policy ICT Information Management and Security Policy

	Intellectual Property Policy Policy Framework Privacy Policy Procurement Policy Records and Information Management Policy Student Communication Policy Student Expectations and Responsibilities Policy Student General Conduct Policy
Related Procedures	Children on Campus Procedure Commercialisation of Intellectual Property Procedure Employee Family and Domestic Violence Support Procedure Integrated Planning and Performance Procedure Intellectual Property Procedure Records and Information Management Procedure Student Communication Procedure
Related forms, publications and websites	
Definitions	**Terms defined in the Definitions Dictionary**
	Employee A person employed by the University and whose conditions of employment are covered by the Enterprise Agreement and includes persons employed on a continuing, fixed term or casual basis. Employees also include senior Employees whose conditions of employment are covered by a written agreement or contract with the University. Family and Domestic Violence Family and Domestic Violence means violent, threatening or other abusive behaviour by certain individuals known to an Employee that

both seeks to coerce or control the Employee, and causes them harm or fear.

Policy

A high level strategic directive that establishes a principle based approach on a subject. Policy is operationalised through Procedures that give instructions and set out processes to implement a Policy.

Student

A person who is enrolled in a UniSQ Upskill Course or who is admitted to an Award Program or Non-Award Program offered by the University and is: currently enrolled in one or more Courses or study units; or not currently enrolled but is on an approved Leave of Absence or whose admission has not been cancelled.

University Members

Persons who include: Employees of the University whose conditions of employment are covered by the UniSQ Enterprise Agreement whether full time or fractional, continuing, fixed-term or casual, including senior Employees whose conditions of employment are covered by a written agreement or contract with the University; members of the University Council and University Committees; visiting, honorary and adjunct appointees; volunteers who contribute to University activities or who act on behalf of the University; and individuals who are granted access to University facilities or who are engaged in providing services to the University, such as contractors or consultants, where applicable.

Definitions that relate to this policy only

Availability

Ensuring that authorised Users have access to information when required.

Confidentiality

Ensuring that information is only accessible to those with authorised access.

ICT Resources

All of the University's Information and Communication Technology Resources and facilities including, but not limited to : mail, telephones, mobile phones, voice mail, SMS, facsimile machines, email, UConnect, MyStaffDesk, the intranet, computers, printers and multi-

	function devices, scanners, access labs or other facilities that the University owns, leases or uses under Licence or by agreement, any off campus computers and associated peripherals and equipment provided for the purpose of University work or associated activities, or any connection to the University's network, or use of any part of the University's network to access other networks. **Integrity** Safeguarding the accuracy and completeness of information and processing methods. **Supervisor** Any person responsible for leading the activities or others. In the context of this policy, a Supervisor includes Employees at any classification level or title who have responsibilities for leading, managing or supervising work teams and/or individual Employees. **User** Refers to all University Members, any person enrolled in an award course of study at the University and any person registered to attend short courses, seminars or workshops in any unit of the University as well as all other persons including members or the general public, who have been granted access to, and use of, the University's ICT Resources. A member of the public reading public University web pages from outside the University is not by virtue of that activity alone considered to be a User.
Keywords	
Record No	13/230PL