Acceptable Use of ICT Resources - Governing Policy

1. Purpose of policy

1.1 This policy sets out what is acceptable use of the University's Information and Communication Technology (ICT) resources, and the University's expectations of all users ('clients'), in respect to:

(a) the provision of resources;

(b) access to resources;

(c) ethical, responsible and legal use of resources; and

(d) privacy and confidentiality when using resources.

1.2 It also addresses the implications for breaches of this policy.

2. Policy scope and application

2.1 This policy applies to all 'clients' of University ICT resources.

2.2 It is the individual responsibility of each client of the University's ICT resources to comply with this policy and associated procedures, as a condition of such access.

2.3 Clients' personal use of University-provided ICT services, facilities and devices including where Clients' personal devices are used to access University email/Wi-Fi etc., is in scope.

3. Definitions

Please refer to the University's Glossary of Terms for policies and procedures. Terms and definitions identified below are specific to this policy and are critical to its effectiveness:

Clients includes Staff, Student or Affiliates who, based on their relationship with the University, need access granted to University ICT resources.

Staff are defined as individuals who hold an active employment contract with the university and are present in the University's Human Resources and Payroll System.

A Student is defined as an individual who is currently enrolled in a program at the University. However, where explicitly stated, student may include an applicant to the University, a student on a leave of absence, or a former student (alumni) who has completed their program and are present in the University's Student Information System.

An Affiliate is defined as an individual who has a bona fide relationship with the University for which approval has been gained to offer access to various ICT resources. This may include adjunct or visiting appointees, volunteers, contractors and consultants.

ICT Resources includes a range of information and communication technology hardware, software and services that may be owned, contracted, licensed, managed or otherwise facilitated by the University for use by the University and its authorised clients.

4. Principles

4.1 Provision of resources

4.1.1 The University provides significant ICT resources to support the University's academic programs, research endeavours, community engagement and administrative services.

4.1.2 The integrity and the security of the University's ICT resources are of critical importance to the University's business continuity and reputation. As such, all resources are managed in accordance with appropriate ICT and organisational standards.

APPROVAL AUTHORITY

Council

RESPONSIBLE EXECUTIVE MEMBER

Chief Operating Officer

DESIGNATED OFFICER

Director, Information Technology

FIRST APPROVED

3 February 1998

LAST AMENDED

10 December 2019

REVIEW DATE

3 December 2024

STATUS

Active

4.1.3 Unauthorised access to, or interference with, ICT resources may jeopardise the University and is strictly forbidden. This includes the installation of unauthorised software and/or hardware onto University networks or systems, or use of unauthorised games, or other content unrelated to legitimate University purposes via the University network.

4.1.4 Staff should use the designated University email system in the course of sending and receiving any communications related to University business and must not use private email accounts for any University related purposes.

4.1.5 Cost centres are responsible for staff use of telephone services. Service costs will be charged to cost centres to ensure financial responsibility.

4.2. Authorised access to resources

4.2.1 The relevant University organisational unit shall determine who has access to ICT resources.

4.2.2 Clients are responsible for their own accounts and are permitted to access only those resources for which they have been authorised. No client should ever allow any other person to use their password or login to access any system.

4.2.3 No client shall, under any circumstances, take any action that would or might lead to circumventing or compromising security of the University's ICT resources.

4.2.4 The University takes a centralised approach to software asset management. The University will only use a genuine copy of legally acquired software that is configured and used in accordance with the licence terms and conditions as set out by the copyright holder. The making or use of unauthorised or illegal software copies is prohibited.

4.2.5 The University deploys a Managed Operating Environment (MOE) to all client computing systems in the designated environment to deliver a stable, supportable and secure platform for University related activity. The Director, Information Technology is responsible for the signing of software licence agreements, development and implementation of controls, procedures and standards to implement this centrally. Exceptions to the MOE and permission to self-install software are subject to approval by the Cost Centre Manager and the Director, Information Technology.

4.3. Ethical conduct and responsible use

4.3.1 Expectations of acceptable use of ICT resources are based on the ethical principles set out in the Staff Code of Conduct - Governing Policy and the Student Conduct - Governing Policy, and with reference to the Student Charter. Staff, students and affiliates are expected to exercise responsibility; use resources appropriately and efficiently; respect the rights and privacy of others; and operate within the laws of the State and Commonwealth, and the policies and procedures of the University.

4.3.2 Clients are expected to demonstrate respect towards all persons. Behaviours such as defamation, discrimination, vilification, bullying and harassment are not only inconsistent with University policies and procedures but may also result in legal action. Clients found to be intentionally accessing, downloading, storing or distributing pornography will be subject to disciplinary action for serious misconduct.

4.3.3 Clients must respect the laws in relation to copyright and moral rights of authors/creators of literary, dramatic, artistic and musical works and all audio-visual media. Clients should familiarise themselves with the principles of the Intellectual Property – Governing Policy and Copyright – Governing Policy, and avoid using ICT resources to use, obtain or distribute copyright content without permission.

4.3.4 Clients should limit personal use of ICT resources to incidental, infrequent and brief and should avoid conflicts of interest.

4.4. Information privacy and confidentiality

4.4.1 Staff of the University, which is constituted under an act of state parliament, are bound by the *Public Sector Ethics Act 1994 (Qld)*. As such, staff should have no expectation that their UniSC email accounts or web-browsing activities, or similar, are personal or private. Staff should be aware that all use of ICT resources may be monitored and recorded and may take appropriate actions if misuse of these resources is identified.

4.4.2 Clients who have authorised access to systems and data containing personal information about staff, students, or other individuals (including, but not limited to, research subjects and patients), or confidential information of the University, must maintain the confidentiality of the information to which they have access in accordance with the *Information Privacy Act 2009 (Qld)*, the *Privacy Act 1988* (Cth), University policies and procedures, and where relevant contractual obligations.

4.5. Compliance and Monitoring

4.5.1 The University reserves the right to monitor aspects of its information systems and network usage.

4.5.2 Any breaches of this policy, by any individual, should be brought to the immediate attention of the Director, Information Technology. This includes data breaches, even if inadvertent or accidental, which involve unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, as this may need to be notified to affected individuals and relevant authorities.

4.5.3 Breaches of this policy may be referred for investigation as possible misconduct or serious misconduct under relevant University policies and procedures, including the Staff Code of Conduct – Governing Policy, and the Student Conduct - Governing Policy.

4.5.4 The University reserves the right to restrict access by a client when faced with evidence of a breach of University policies and/or law.

4.5.5 Where required by law, the University will refer any potential breach to the relevant law enforcement authority and will report any potential breach which may amount to corrupt conduct to the Queensland Crime and Corruption Commission.

END

RELATED DOCUMENTS

• Acceptable Use of ICT Resources - Procedures

• Adopting Cloud-based Services - Procedures
• Anti-Discrimination and Freedom from Bullying and Harassment - Governing Policy
• Copyright - Governing Policy
• Copyright - Procedures
• ICT Security - Operational Policy
• Information System Operations - Procedures
• Intellectual Property - Governing Policy
• Intellectual Property: Commercialisation - Procedures
• Intellectual Property: Commercialisation Revenue - Procedures
• Intellectual Property: Student IP - Procedures
• Intellectual Property: Transfer of Rights to Creators - Procedures
• Social Media - Operational Policy
• Social Media - Procedures
• Student Conduct - Governing Policy

LINKED DOCUMENTS

• Acceptable Use of ICT Resources - Procedures

SUPERSEDED DOCUMENTS

• Software - Governing Policy
• Telephone - Managerial Policy
• Electronic Mail - Managerial Policy

RELATED LEGISLATION / STANDARDS

• Right to Information Act 2009 (Qld)
• Public Records Act 2002 (Qld)
• Public Sector Ethics Act 1994 (Qld)
• Queensland Information Standards
• Copyright Act 1968 (Cth)
• Privacy Act 1988 (Cth)
• SPAM Act 2003
• Information Privacy Act 2009 (Qld)
• Student Charter