Information and Communication Technology Policy

Section 1 - Purpose and Scope

(1) The University of Queensland (UQ or the University) is committed to providing Information and Communication Technology (ICT) resources to support, enable and enhance its activities.

(2) This Policy:

a. outlines acceptable use (and misuse) of UQ ICT resources;
b. supports UQ through effective provisioning and management of ICT resources; and
c. seeks to protect UQ's reputation and safeguard its resources.

(3) This Policy should be read in conjunction with other ICT policies and procedures (see associated information).

Scope

(4) This Policy applies to consumers of UQ ICT resources or UQ information including, but not limited to:

a. Students
b. Staff
c. Contractors and consultants
d. Visitors
e. Affiliates and third parties.

(5) Consumers that are connected to UQ networks or services must comply with this Policy, irrespective of location or device ownership (e.g. personally-owned computers). The Chief Information Officer must approve exceptions to this Policy.

Section 2 - Principles and Key Requirements

(6) ICT is of critical importance to UQ activities. All consumers of UQ ICT resources are expected to use these facilities and services appropriately and reasonably.

Access to ICT Systems and Resources

(7) Access to ICT systems and resources is provided to consumers for carrying out University work, study, or for other UQ purposes. UQ incurs costs in providing ICT systems and resources, and access is not provided to consumers unconditionally. The following conditions apply:

a. Consumers must not share account login details such as usernames or passwords.
b. Passwords should be secure. Password recommendations are included in the section 6 Appendix.
c. Staff access to UQ ICT systems and resources is terminated when employment with UQ ceases. Account access may be extended in some circumstances. Visit the Keeping staff email after you leave UQ webpage for more

information.

d. UQ reserves the right to limit, suspend or remove access where necessary.
e. UQ will take appropriate steps to ensure Internet access is granted to minors in compliance with legislative requirements.
f. UQ will endeavour to make online services accessible in alignment with industry best practices and accessibility guidelines.
g. Administrator access to UQ computers will only be granted where necessary and with appropriate approval.
h. Passwords less than 12 characters must be changed every 12 months. Passwords greater than 12 characters must be changed every 24 months.

Software

(8) Software licensed to UQ (UQ Licensed Software) must only be used for purposes legitimately associated with UQ's operations and in accordance with the relevant software licence terms. This includes online services (i.e. software-as-a-service) licensed to UQ.

(9) Consumers must not install software on UQ devices that is not appropriately licensed to UQ.

(10) The following conditions of use are intended to inform consumers of their responsibilities when using UQ Licensed Software and to minimise UQ's risks of copyright infringement, or other breaches of software licence terms:

a. All UQ Licensed Software will only be used in compliance with the applicable licence terms and conditions.
b. Consumers should be aware of and comply with the terms and conditions of any software that is being used.
c. Delegates identified within the Contractual Delegations Policy are the only individuals at UQ that are authorised to approve software agreements on behalf of the University.
d. Information and communication technology procedures outline roles and responsibilities of IT staff and consumers when purchasing and installing software.
e. UQ Licensed Software must not be installed on personally-owned devices, unless explicitly permitted in the applicable licensing agreement and by management.
f. Installation files for UQ Licensed Software must not be unlawfully copied, and unlawfully copied software must not be used or installed on UQ devices.
g. UQ Licensed Software master media and licence keys (where applicable) should be securely stored in order to avoid theft or unauthorised use or copying.

Acceptable Use of ICT Resources

(11) UQ requires all consumers of its ICT resources to do so in an authorised, responsible, ethical, equitable and legal manner and in accordance with the UQ Staff Code of Conduct Policy and Student Code of Conduct Policy. Incidental personal use of University ICT resources is permitted. Such use must be kept to a minimum.

(12) While UQ acknowledges that exceptions may exist under certain circumstances, unauthorised use of ICT resources may lead to increased cost, risk, and reputational damage to UQ. Consumers should be aware that UQ ICT resources must not be used:

a. for gambling purposes;
b. in a manner that constitutes an infringement of copyright; or
c. to access, store or transmit pornographic, racist, violent, or any other unacceptable material.

(13) Consumers' use of UQ's ICT systems and resources may be monitored (see section 4 of this Policy).

Misuse of UQ ICT Resources

(14) The Chief Information Officer may authorise an investigation into alleged misuse. If allegations are deemed to be valid and of a serious nature, evidence of misuse will be reported to the appropriate body:

a. If the consumer is a staff member – formal disciplinary action may occur in accordance with the Misconduct/Serious Misconduct clauses outlined in the Enterprise Agreement. The case may also be referred to the Integrity and Investigations Unit.
b. If the consumer is a student – the information may be reported to Student Integrity and Misconduct in accordance with the Student Integrity and Misconduct Policy.

Email and Bulk Messaging

(15) UQ recognises the importance of email for efficient communication. Unauthorised use of email can result in security risks and reputational damage. The measures below apply to consumers of UQ ICT resources.

a. Information Technology Services will maintain the official email system for UQ, internally or through an agreement with an external service provider.
b. If an Organisational Unit wishes to maintain its own email server, approval must be obtained from the Chief Information Officer.
c. A UQ email address must be used for the delivery of all official UQ email.
d. Staff must not use external email accounts (e.g. Gmail, BigPond or Hotmail) for UQ correspondence.
e. Retiring academic staff are eligible to retain access to their email account when employment with UQ ceases. Accounts with no activity for a period of 12 months will be suspended.
f. Students, Alumni, volunteers, Academic Title Holders and Honoraries may forward their UQ email to another account or provider. Staff email accounts must not be forwarded to an external provider without approval which must be signed by the head of the Organisational Unit or their delegate.
g. UQ may communicate to its staff and students, through its authorised managers, information which:
    i. is relevant to UQ as a whole (e.g. to all UQ or large groups of staff or students) or to particular sections of the UQ such as Faculties, Schools or Divisions; and
    ii. is required for the effective functioning of the University or the relevant organisational unit; or which covers issues, policies, corporate events or decisions with a direct connection to the work of the University and its key organisational units.
h. Consumers must not send messages to a large number of recipients (e.g. all staff, all students, alumni, or a large volume of external users) without approval, as outlined in the Email and Bulk Messaging Procedure.
i. Consumers may delegate mailbox access when required. If a consumer is unable to delegate mailbox access, authorisation must be provided by the Chief Information Officer.

Digital Presence

(16) UQ's digital presence includes websites, web applications, mobile applications and other means of providing information and services online. UQ's digital presence must:

a. comply with relevant legislation and UQ's policies and procedures;
b. meet the needs of consumers;
c. be cohesive and consistent; and
d. be accurate and up-to-date.

(17) UQ will create and maintain its digital presence in accordance with the UQ Digital Presence Procedure.

Information Management and Cyber Security

(18) UQ seeks to respect the privacy and confidentiality of consumers and protect its information and assets. The following policies cover these matters:

a. Information Management Policy
b. Cyber Security Policy
c. Privacy Management Policy.

(19) All UQ computers, laptops, and tablets (where possible) must have UQ's anti-virus software installed. If a computer is unable to run UQ's anti-virus software it presents a security risk and must not be used to access UQ's ICT resources or information. Any exceptions must be made using the Cyber Security Exceptions Procedure.

Section 3 - Roles, Responsibilities and Accountabilities

Consumers of UQ ICT Resources

(20) Consumers are responsible for being aware of and complying with this Policy. Consumers should also be aware that:

a. use of UQ ICT resources is subject to Australian laws and other relevant UQ policies. This includes but is not limited to copyright, breach of confidence, defamation, privacy, contempt of court, bullying and cyber-bullying, harassment, vilification, anti-discrimination, wilful damage and computer hacking; and
b. access to some third party applications and content has separate contractual arrangements and terms and conditions, which may apply over and above this Policy.

(21) It is the responsibility of consumers to check and maintain their UQ email account regularly.

Information Technology Staff

(22) Information Technology staff are responsible for:

a. provisioning ICT resources (e.g. consumer accounts, file storage, access to systems);
b. monitoring the use of resources to determine violations of authorised use;
c. technical enforcement of this Policy including:
    i. preventing and monitoring access to inappropriate content;
    ii. suspending consumer access when required and approved by Chief Information Officer; and
d. complying with local standard operating procedures where applicable.

Chief Information Officer

(23) The Chief Information Officer is responsible for:

a. ensuring that IT staff members are resourced to investigate alleged misuse;
b. authorising the suspension of consumer accounts following investigations of misuse; and
c. ensuring this Policy is enforced and maintained.

Section 4 - Monitoring, Review and Assurance

(24) To improve services and protect consumers, UQ reserves the right to monitor access and usage of all UQ ICT systems and resources. Consumers should be aware that use of UQ ICT resources, including email, is not considered private, and that UQ may monitor, access, restrict, terminate or suspend accounts with approval from the Chief Information Officer or their delegate.

(25) UQ will meet its data retention obligations under the Telecommunications (Interception and Access) Act 1979 (Cth).

Section 5 - Recording and Reporting

(26) All usage (e.g. email, hard drives, or network use) may be recorded for the purposes of security and risk management (e.g. backups, performance monitoring, or compliance requirements).

(27) Consumers who become aware of possible breaches of this Policy must report it to either:

a. Information Technology Services; or
b. The Head of their Organisational Unit.

(28) Breaches of this Policy may be reported to UQ's Information Technology Governance Committee, the Chief Information Officer, the Chief Human Resources Officer or to the appropriate external authorities, which may result in civil or criminal proceedings.

Section 6 - Appendix

Related Policies

(29) Information Management Policy

(30) Cyber Security Policy

(31) Privacy Management Policy

Related Legislation

(32) Telecommunications (Interception and Access) Act 1979 (Cth)

(33) Privacy Act 1988 (Cth)

Definitions

Term	Definition
Consumer	All staff, students, visitors, contractors, third parties, clinical and adjunct title holders, affiliates, alumni and all other people who access UQ's systems, networks or other ICT resources.

Term	Definition
UQ ICT resources	any UQ IT system or asset, including but not limited to: • Networks (wireless and wired) • Property and facilities • Equipment whether owned or leased by UQ including telephony, computers, servers, storage, including its associated hardware and software • UQ websites and systems (applications) • Data, information and video • Accounts.
ITS	Information Technology Services.
SITC	Strategic Information Technology Council.
ITGC	Information Technology Governance Committee.
Unacceptable material	Includes materials not related to delivery of UQ's core purpose or its effective operations, including but not limited to: • Pornography • Violent content • Racist content • Gambling or content relating to gambling • Viruses and malware • Games. Unacceptable material excludes material that is permitted under UQ's principles for freedom of speech or academic freedom, as set out in the UQ Governance and Management Framework.
Software	Includes, but is not limited to, purchased or commercial software, sound, graphics, images, or datasets; shareware; freeware; and electronically stored documentation and the media that holds it. This includes online services (i.e. software-as-a-service) licensed to UQ. Not included in this definition are non-copyrighted computer data files that have no significance beyond the individual or organisational unit.
Software Licence compliance	Clear documentation that the number of legally obtained and genuine software licences matches the number of installed instances of a given software product on the University's systems or devices.

Password Recommendations

(34) When choosing a password:

a. Use at least 10 characters including at least 1 letter and 1 number or special character. Approved special characters include: # $ % ' ( ) * + , - / : ; < = > [ ] ^ _ ` { | } ~
b. Do not use your name, phone number, date of birth or other identifiable information.
c. Do not use a password you have used previously.

Suggestions for a Strong Password

a. Use three or four unrelated words with some non-alphabetic characters and capitalised characters. Try to create a phrase that is easy to remember, but difficult to guess.
b. Avoid using personal information. This includes your maiden name, car registration number, address or family member's name.
c. Avoid duplicating characters (aaabbbccc) or keyboard patterns (qwertyuiop). These can easily be seen by someone watching you type.

Status and Details

Status	Historic
Effective Date	14th December 2021
Review Date	13th May 2022
Approval Authority	Provost and Senior Vice-President
Approval Date	14th December 2021
Expiry Date	10th April 2024
Policy Owner	Marni Jacoby Chief Information Officer
Enquiries Contact	Information Technology Services