INFORMATION AND COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE POLICY AND PROCEDURE

CONTENTS

1 PURPOSE

1.1 This policy and procedure sets out CQUniversity's expectations and requirements for the use of its information and communications technology (ICT) resources, including network, devices, and services, including externally hosted or cloud-provided services by its users, as well as what CQUniversity can do with the information it holds.

2 SCOPE

2.1 This policy and procedure applies to individuals (users) accessing CQUniversity-owed ICT resources, including:

- employees, students, and Council and Committee members
- employees and students of CQUniversity's controlled entities
- other affiliated individuals including contractors, service providers, and other members of the University's supply chain who are provided access to the University systems or data as required to deliver contracted services, and
- visitors such as members of the public or community.

3 POLICY STATEMENT

3.1 The University provides its Council and Committee members, employees, and students with access to ICT resources to enhance their ability to work and study. The University may also provide other affiliated individuals and visitors with access to ICT resources to enhance their ability to complete tasks for, liaise with, or otherwise engage with the University.

3.2 Individuals that use the University's ICT resources and to whom this policy and procedure applies will be known as 'users'. All users must comply with this policy and procedure, and any legislation, regulations, and policy documents applicable to using the University's ICT resources.

3.3 ICT resources must be used in an efficient, lawful, and ethical manner consistent with the employee Code of Conduct, Student Email Account Policy and Procedure, Student Behavioural Misconduct Procedure, and policy documents relevant to using the University's resources.

3.4 University employees are considered to be public sector employees. As such, the principles of the Queensland Government's Use of ICT Services, Facilities and Devices Policy (IS38) apply, in particular:

a) use and/or access to these resources must be able to survive public scrutiny and/or disclosure

b) information must only be transmitted or made available using these resources under University approved protocols, and

c) limited personal use is permitted, provided that such use is infrequent and brief, and does not contravene University policy documents or State or Commonwealth laws; interfere with official use of information technology systems; interfere with an employee's obligations to the University; or be used to conduct a personal business.

3.5 The University is able to collect, hold, use and disclose personal information of users to enable the University to meet its legal obligations and for a range of University purposes.

4 PROCEDURE

ICT access and use

4.1 Employees and students who do not ordinarily have access to ICT resources will be able to access ICT resources at University campuses for work-related or study activities.

4.2 Employees who have ceased employment with the University will be able to access University resources at the University's discretion.

4.3 The intentional viewing, storage, display, or distribution of adult content is strictly prohibited, and instances of this occurring will be dealt with as a breach of this policy and procedure, except for cases where an explicit exception has been made.

University owned devices

User responsibilities

4.4 Users must report to the Technology and Services Assistance Centre (TaSAC):

a) known security breaches and risks

b) damage, hardware and software faults, and

c) Stolen or lost hardware items.

4.5 If a user is allocated a device, they will be recorded as its custodian. They accept full responsibility for its proper use and care. This includes all accessories and cables.

4.6 Any activities conducted with that device should be able to survive public scrutiny and/or disclosure.

a) Device misuse that causes loss or requires repair may require the user to contribute to the cost.

b) Device use that incurs additional charges, such as unintended purchases or excessive data charges, may require the employee to contribute to the cost.

c) Device misuse that incurs a fine, infringement, or other penalty will be the user's responsibility.

4.7 Users are responsible for ensuring devices have their security and software regularly updated.

4.8 Users are responsible for ensuring data is not stored on local devices and hard drives unless it is backed up or synchronised with a recommended University service that has been reviewed for suitability and cybersecurity. Recommended practice for working with University data is to store it in the following places:

a) Microsoft OneDrive within the University's Microsoft Office 365 environment

b) University provided network drives

c) AARNet Cloudstor file sharing service

d) data storage locations specified in the Research Data Management Policy and Procedure for researchers and research higher degree students.

4.9 University devices, including SIM cards, will remain University property. If a user ceases to have a relationship with the University, they must return all devices, accessories, and cables, to the Digital Services Directorate.

a) If the returned device is not considered by the University to be in good order, the cost of repair or replacement may be deducted from outstanding benefits or entitlements available to the user.

b) If the device is not returned, the user may be charged the cost of its replacement. The device will be treated as stolen and will be cancelled, remotely locked, or remotely erased.

c) Departing employees may request to retain their mobile phone number. The Digital Services Directorate will provide the necessary transfer paperwork; however, the departing employee is responsible for transferring the existing phone number to a personal account. If the phone number has not been transferred by the agreed transfer date, the University will cancel the phone number.

4.10 If a device is no longer required, it will be returned to the Digital Services Directorate.

Purchasing and replacement

4.11 The Digital Services Directorate manages a preferred supplier contract on behalf of the University and will use the preferred supplier to purchase ICT resources and accessories, and manage voice and data plans. The Digital Services Directorate maintains a record of current charges and data rates for such devices.

4.12 All purchases of ICT resources, including voice and data plans, must be made through TaSAC.

4.13 ICT resources and equipment will be replaced due to business requirements, technology changes, or device lifecycle e.g. end of warranty, and will be done at the discretion of the Digital Services Directorate. Additional approval from a delegated approver may be required from time to time.

4.14 All purchases/subscriptions of software, devices or accessories, servers, externally hosted services, or cloud services will be made with review and approval from the relevant financial delegated approver.

4.15 Employees will be allocated one computer that is fit for purpose of the business requirements. Previous devices nominated for replacement will be removed and disposed in line with existing practices and will be irrespective of the purchasing school/department or project.

4.16 Incoming employees may transfer their existing mobile phone number to the University's account if their request is approved by a delegated approver. Any costs associated with such transfers, such as a cancellation of contract fee, will be borne by the incoming employee.

Use of student's personal information

4.17 The University can use student's personal information in accordance with University policy documents. The University may monitor, collect, hold, use and disclose a student's personal information to enable the University to meet its legal obligations and for a range of internal University purposes. These include but are not limited to administering a student's admission, enrolment, academic progress and academic integrity, disciplinary matters, the investigation of academic integrity and/or academic misconduct matters, graduation, accommodation, access to University facilities and services, library loans, fees, visa, immigration, taxation and financial support purposes.

Personal devices

4.18 The University permits users to connect their own personal devices to the University network or another device. Examples of another device would be a USB external hard drive or personal phone being connected to a University owned computer.

4.19 Users who connect a personal device to the University network or another device must ensure that their devices are secure and have taken all reasonable steps to prevent any cybersecurity threat.

4.20 Users of personal devices must adhere to this policy and procedure when connected to any University network or another device and agree that:

a) any University data stored on personal ICT devices remains the sole property of the University

b) they have an obligation to protect the security of that data, and

c) at the end of employment or studies at the University, users must remove all University data and software from personal devices, while ensuring the University has retained a copy of that data.

4.21 The following minimum requirements must be met before users connect any personal devices to the University network or device:

a) to prevent unauthorised access, devices must be password protected using the features of the device. Where possible, they must be configured to automatically lock with a password or PIN after an idle period

b) the device's operating system must be current with security patches and updates applied, as released by the manufacturer

c) the device must be capable of connecting to the University enterprise wireless networks

d) suitable anti-virus (AV) protection must be installed on the device. The AV software installed must be from a reputable vendor and up-to-date, and

e) 'Jailbroken' devices are strictly forbidden from accessing the University network, as are devices with any unlicensed or pirated operating systems, as they represent an unacceptable cybersecurity risk.

4.22 The University may monitor use of personal ICT devices connected to its network or devices. This information may be collected and archived, will be held subject to law enforcement or other legally binding access requirements, and may be subject to public access.

4.23 The University is not responsible for:

a) any inconvenience users may experience in connection with using personal ICT devices to access University ICT facilities. University-provided ICT support will be strictly limited to connecting personal ICT devices to the University network.

b) any costs associated with personal ICT devices. The University will not reimburse users for any voice or data charges, software or application acquisition fees, support, or insurance costs associated with personal ICT devices, and

c) any personal loss or damage users may suffer by University actions undertaken to protect University data stored on personal ICT devices, including enforcing a remote wipe of the device.

Cybersecurity, monitoring and filtering

4.24 The University reserves the right to monitor, record and maintain logs, in relation to any and all aspects of its ICT systems and devices. Information captured as part of monitoring, recording and maintaining logs may be used to assist with, but is not limited to, determining if a user is acting unlawfully, is in violation of this and any other University policy documents, an investigation into academic integrity/misconduct matters, research and planning improvements for the University. Additionally, the University may use such information to meet legal obligations.

4.25 Where abnormal activity is detected or a complaint has been made, users may be called upon to explain their use of ICT resources.

4.26 The University will enforce system and device settings where necessary to reduce cybersecurity risk, while taking into consideration business requirements.

4.27 The University cybersecurity officers will reduce cybersecurity and business risk by investigating content, blocking, filtering, and threat removal. This may include and is not limited to:

a) removal of email from employee and student mailboxes

b) blocking websites, such as adult content

c) blocking email address or domains, and

d) stopping transmission and storage of certain types of data, such as credit card information.

4.28 Applications can be made to TaSAC for exemption from certain filtering and blocks.

a) For adult content, applications must include approval from the Human Research Ethics Committee and relevant supervisor. Those currently exempt are researchers, academics, teachers, or students, whose area of research or teaching involves adult content.

4.29 The University may review the contents of ICT resources, including email or logged information. These actions require approval from the Director, People and Culture Directorate (regarding employees) or Director Governance (regarding students) to support alleged/suspected misconduct or data requests to meet legislative or legal obligations.

4.30 If an employee is absent on unexpected or approved leave, or otherwise ceases employment, the University may arrange alternative employee access to the absent employee's email and/or file storage to ensure that University business operations are not disrupted.

Communication

Email distribution lists

4.31 Email is provided for teaching, learning, research, consultation, and administrative purposes. The University maintains email distribution lists to provide formal and informal channels of communication.

4.32 The official employee mailing list is official@lists.cqu.edu.au and is the official means of distributing messages and information to employees. All employees must maintain membership of this mailing list. The ability to post to this list is restricted and moderated by Corporate Communications and TaSAC.

StaffNet

4.33 StaffNet is the University's intranet and preferred medium for general communications, campus news, and service announcements.

Breaches

4.34 Breaches of this policy and procedure may result in user access being revoked and will be dealt with as follows:

a) **CQUniversity employees**: may be treated as an alleged breach of the employee Code of Conduct, which may involve alleged misconduct or serious misconduct. Any disciplinary action will be managed in accordance with the Central Queensland University Enterprise Agreement

b) **CQUniversity students**: may be treated as alleged student misconduct. Any disciplinary action will be managed in accordance with the Student Behavioural Misconduct Procedure, Student Academic Integrity Policy and Procedure, Research Higher Degree Integrity Policy and Procedure or other relevant policy document

c) **CQU Executive Business Training employees and students:** will be managed under CQU Executive Business Training's policy documents

d) **Other individuals, including visitors**: will have their ICT access rights revoked. If appropriate, further action may be taken in accordance with relevant policy documents or legislation.

5 RESPONSIBILITIES

Compliance, monitoring and review

5.1 The Deputy Vice-President (Digital Services) is responsible for implementing, monitoring, reviewing, and ensuring compliance with this policy and procedure.

Reporting

5.2 No additional reporting is required.

Records management

5.3 Employees must manage records in accordance with the Records Management Policy and Procedure. This includes retaining these records in a recognised University recordkeeping information system.

5.4 University records must be retained for the minimum periods specified in the relevant Retention and Disposal Schedule. Before disposing of any records, approval must be sought from the Records and Privacy Team (email records@cqu.edu.au).

6 DEFINITIONS

6.1 Terms not defined in this document may be in the University glossary.

Terms and definitions

Adult content: pornography or any media or material that could be interpreted as pornography.

Affiliated individual: any person who is not a CQUniversity student or employee

Delegated approver: an employee with authority to make decisions regarding an individual's use of a University-funded ICT resources and equipment. Delegated approvers are:

Category of individual	Delegated approver
Senior executive	Vice-Chancellor and President
Educators	Vice President (Academic)/Dean of School
Professional employee	Senior Executive/Deputy Vice-President/Director/Dean of School

Devices or University-owned devices: any desktop, laptop and tablet computers or mobile phones, modem, iPad, mobile tablet, Internet of Things (IOT) device or any other emerging voice or data device that accesses the University network or a commercial mobile telecommunications service that the University has purchased and provided to individuals to use for official University business.

Internet: references to the internet include the University intranet or network.

Jailbroken: the process of hacking devices to bypass Digital Rights Management restrictions, allowing 'unauthorised' software to be run or make other changes to the operating system.

Users: individuals that use the University's ICT resources including CQUniversity employees, students, Committee and Council members, CQU Executive Business Training Centre employees and students, visitors and other affiliated individuals who are provided access to deliver contracted services.

7 RELATED LEGISLATION AND DOCUMENTS

Central Queensland University Enterprise Agreement 2017

Code of Conduct

Copyright Act 1968 (Cwlth)

Cybercrime Act 2001 (Cwlth)

Intellectual Property and Moral Rights Policy

Intellectual Property Laws Amendment Act 2015 (Cwlth)

Procurement Policy and Procedure

Research Data Management Policy and Procedure

Research Higher Degree Integrity Policy and Procedure

Spam Act 2003 (Cwlth)

Student Behavioural Misconduct Procedure

Student Email Account Policy and Procedure

Use of ICT Services, Facilities and Devices Policy (IS38) (Queensland Government Enterprise Architecture)

8 FEEDBACK

8.1 Feedback about this document can be emailed to policy@cqu.edu.au.

9 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Vice-Chancellor and President
Delegated Approval Authority	N/A
Advisory Committee	University Management Committee
Administrator	Deputy Vice-President (Digital Services)
Next Review Date	20/04/2024

Approval and Amendment History	Details
Original Approval Authority and Date	Vice-Chancellor's Advisory Committee 09/09/2015
Amendment Authority and Date	Planning and Development Committee 09/01/2004; Vice-Chancellor and President 1/05/2006; Vice-Chancellor and President 31/01/2007; Vice-Chancellor and President 13/08/2007; Vice-Chancellor and President 19/07/2011; Terminology update 4/01/2012; Periodic review and update 28/07/2015, including adding BYOD, CQU owned devices; Vice-Chancellor and President 09/09/2015; Vice-Chancellor and President 7/08/2018; Acting Senior Deputy Vice-Chancellor (International and Services) 16/10/2018; Vice-Chancellor and President 20/04/2021; Editorial amendments 05/01/2023.
Notes	This document consolidated and replaced the Acceptable Use of Information and Communications Technology Facilities and Devices Policy and Procedure and the Mobile Device Principles (approved 7/08/2018).