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, external tenants and partnerships, and other members of the University's supply chain who are provided access to the University systems or data as required, 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 Account Policy and Procedure, Student Conduct Policy and Procedure, Council Charter and policy documents relevant to using the University's resources.

3.4 University employees are considered 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 ICT systems; interfere with an employee's obligations to the University; or be used to conduct a personal business.

3.5 The University may collect, hold, use and disclose personal information of users where necessary and relevant to the University's functions and activities and/or to meet legal obligations. Refer to the Privacy Policy and Procedure for further information.

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 Employees who are on extended leave (greater than five weeks) must return ICT devices to their supervisor or a Digital Services employee on campus, and their University account will be disabled unless an exemption is approved by the Executive Director People and Culture.

4.4 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. Refer to section 4.31 for information on seeking an exemption to certain filtering or blocks.

University owned devices

User responsibilities

4.5 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, lost or seized hardware items.

4.6 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.

4.7 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.

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

4.9 Users must ensure 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. Records should also be stored as per the Records Management Policy and Procedure. Recommended practice for working with University data is to store it in the following places:

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

b) University provided network drives, or

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

4.10 University devices, including SIM cards, 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 in accordance with the Employee Departure Checklist (for employees) or via their primary University contact (for all other users).

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.

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

Purchasing and replacement

4.12 The Digital Services Directorate uses a preferred supplier contract on behalf of the University for all ICT resources, accessories and plans, and maintains a record of current charges and data rates for such devices.

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

4.14 ICT resources and equipment will be replaced due to business requirements, technology changes, or device lifecycle e.g. end of warranty, at the discretion of the Digital Services Directorate.

4.15 Purchases/subscriptions of software, devices or accessories, servers, externally hosted services, or cloud services can be made with approval from the relevant financial delegate and relevant Digital Services team/s. Refer to the Authorities and Delegations Register for financial delegation limits.

4.16 Employees who work over 0.4 full-time equivalent will be allocated one computer. Previous devices nominated for replacement will be removed and disposed, regardless of the purchasing business area or project.

4.17 User-issued ICT equipment must adhere to the asset management lifecycle. In instances where this process is hindered by employees, the respective business area may be held financially accountable for the replacement cost of the equipment and devices may be disabled if not returned.

4.18 The University supports employees undertaking remote work by providing essential equipment such as a laptop, carrying case, and headset. Employees are expected to independently supply any other accessories for their home office arrangements (e.g. monitors, docking station, keyboard and mouse).

4.19 Incoming employees may transfer their existing mobile phone number to the University's account if their request is approved by the relevant Senior Executive or head of business area. Any costs associated with such transfers, such as a cancellation of contract fee, will be borne by the incoming employee.

Personal devices

4.20 The University permits users to connect their own personal ICT devices to the University network or another device (for example, connecting a USB external hard drive or personal phone to a University owned computer).

4.21 Users who connect a personal ICT 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.

4.22 The University may apply security restrictions to personal ICT devices before allowing devices to access University data.

4.23 When accessing the University network or University-owned services (including externally hosted or cloud-provided services such as email, Microsoft Teams or CQUniversity OneDrive) on personal ICT devices, users agree that:

a) any University data stored on their personal ICT devices remain 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, studies, or affiliation with the University, they must remove all University data and software from their personal devices, while ensuring the University has retained a copy of that data.

4.24 The following minimum requirements must be met before users connect any personal ICT devices to a University network, service 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 protection must be installed on the device. The anti-virus software installed must be from a reputable vendor and up-to-date, and

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

4.25 The University may monitor use of personal ICT devices connected to its network, services 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.

4.26 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

4.27 The University may monitor, review, record and maintain logs of its ICT resources, systems and devices, including email or logged information. Information captured may be used to assist with, but is not limited to, meeting legal obligations, determining if a user is acting unlawfully or in in violation of this or any other University policy document, investigating alleged/suspected integrity/misconduct, and research and planning improvements for the University. The Executive Director People and Culture (for employees), the Director Governance/University Secretary (for students), or primary University contact must approve for data or ICT

resources to be reviewed if relating to alleged/suspected misconduct or to meet legislative or legal obligations.

4.28 Where abnormal activity is detected or a complaint made, users may be required to explain their use of ICT resources.

4.29 The University may enforce system and device settings, including on personal ICT devices, to reduce cybersecurity risk.

4.30 The University cybersecurity officers will reduce cybersecurity and business risk by investigating content, and blocking, filtering, and removing threats. This may include, but is not limited to:

a) removing emails from user and student mailboxes

b) blocking websites, such as adult content

c) blocking email address or domains

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

e) isolating or disabling a user or devices from University systems

f) wiping University data from personal ICT devices, and

g) wiping all data including operating systems, applications, and settings, from University supplied devices.

4.31 Applications can be made to TaSAC for exemption from certain filtering and blocks. Applications to allow adult content must include approval from the Human Research Ethics Committee and relevant supervisor. Those currently exempt from adult content blocking are researchers, academic employees, VET educators, and students whose area of research or teaching involves adult content.

4.32 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

4.33 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.

4.34 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 the Corporate Communications Team and TaSAC.

StaffNet

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

Breaches

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

a) 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) students may be treated as alleged student misconduct. Any disciplinary action will be managed in accordance with the Student Conduct Policy and 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, and

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 Chief Digital Officer 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 University student or employee.

Asset management lifecycle: the sequence of stages an ICT asset goes through, from planning and acquisition to deployment, maintenance, and eventual decommissioning, recycling, or disposal.

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 University employees, students, Committee and Council members, employees and students of CQUniversity's controlled entities, visitors and other affiliated individuals who are provided access to deliver contracted services.

7 RELATED LEGISLATION AND DOCUMENTS

Authorities and Delegations Register

Central Queensland University Enterprise Agreement

Code of Conduct

Copyright Act 1968 (Cwlth)

Cybercrime Act 2001 (Cwlth)

Intellectual Property and Moral Rights Policy

Library Replacement and Repair Charges Procedure

Privacy Policy and Procedure

Procurement Policy and Procedure

Records Management Policy and Procedure

Research Data Management Policy and Procedure

Research Higher Degree Integrity Policy and Procedure

Spam Act 2003 (Cwlth)

Student Academic Integrity Policy and Procedure

Student Account Policy and Procedure

Student Behavioural Misconduct Procedure

Student Conduct 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
Required Consultation	N/A
Administrator	Chief Digital Officer
Next Review Date	21/05/2027

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; Editorial amendments 08/02/2023; Chief Digital Officer 22/05/2023; Editorial amendments 28/02/2024; Acting Vice-Chancellor and President 21/05/2024.
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).