INFORMATION AND COMMUNICATIONS TECHNOLOGY ACCEPTABLE USE POLICY AND PROCEDURE

CONTENTS

1 PURPOSE

1.1 This policy and procedure sets out CQUniversity’s expectations for the use of its information and communications technology (ICT) facilities and devices (resources).

2 SCOPE

2.1 This policy and procedure applies to the University as a corporate entity, CQUniversity Council members, employees and students; all controlled entities; and all other individuals working on the University’s behalf or using University-owned ICT resources.

3 POLICY STATEMENT

3.1 CQUniversity provides its Council members, employees and students, and other individuals, with access to ICT facilities and devices to enhance their ability to perform their work and study. In particular, access to the internet, email and collaborative systems are provided to enable networking and access to worldwide information resources.

3.2 CQUniversity may also provide other individuals (e.g. visitors) with access to ICT resources to enhance their ability to complete tasks for or to liaise with the University.

3.3 All individuals that use CQUniversity's ICT resources and to whom this policy and procedure applies are known as 'users'. All users are required to comply with legislation, regulations and policies applicable to using CQUniversity's ICT resources, including this policy and procedure.

3.4 Council members, employees and students are required to be aware of their obligations set out in this document. Other individuals (e.g. visitors) may be required to read this document as a condition of being issued with a username and password.

3.5 Like all University assets and services, ICT resources must be used in an efficient, lawful and ethical manner consistent with the employee Code of Conduct, the Student Behavioural Misconduct Procedure and policies and procedures relevant to using CQUniversity's resources.

3.6 CQUniversity will take reasonable steps to ensure all users are aware of this policy and procedure and implement measures to reduce risks associated with unacceptable use of and access to ICT resources.

4 PROCEDURE

Using and accessing ICT resources

Access to computers and online facilities for all employees

4.1 Employees who do not ordinarily have access to computers will be able to access computers at CQUniversity campuses for work-related activities and access to online employee facilities, e.g. Employee Self Service Online (ESSO), StaffNet.

4.2 Employees who have ceased employment with the University will be able to access ESSO remotely for up to two years to access payment summaries.

Employee personal use of ICT resources

4.3 CQUniversity 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) ICT facilities and devices, which includes access to the internet and email, are provided for officially approved purposes only

b) use and/or access to these facilities and devices must be able to survive public scrutiny and/or disclosure

c) information must only be transmitted or made available using these facilities and devices under University approved protocols.

4.4 As indicated in IS38, the University will allow employees to use ICT resources for limited personal use, provided that such use is infrequent and brief, does not involve excessive network bandwidth, and does not contravene University policies/procedures or State or Commonwealth laws; interfere with official use of information technology systems; or interfere with an employee's obligations to the University. This condition applies to all forms of personal use, including the use of social networking sites.

4.5 Employees must not use the University's internet access, internal network or computing facilities to conduct personal business. This includes using a CQUniversity VPN connection from home on a personal computer.

Purchasing mobile devices

4.6 CQUniversity provides mobile devices to nominated employees for University-related business communication.

4.7 The Information and Technology Directorate (IaTD) manages a preferred supplier contract on behalf of CQUniversity and will use the preferred supplier to purchase available handsets, devices, and accessories and to manage voice and data plans. IaTD maintains a record of current charges and data rates for such devices.

4.8 All purchases of mobile devices and provision of voice and data plans must be made through the Technology and Services Assistance Centre (TaSAC) by following the CQUniversity Mobile Phones process on StaffNet. Mobile devices must be purchased via IaTD in compliance with the Procurement Policy and Procedure (FMPM). The device (and SIM card if applicable) will remain CQUniversity property.

4.9 Employees must not enter into any device/voice or data plan with any service provider on behalf of CQUniversity, irrespective of device ownership or source of funds, unless prior arrangements have been authorised by the delegated approver and IaTD.

4.10 Incoming employees may transfer their existing mobile number to CQUniversity's account their request is approved. Any costs associated with such transfers, such as a cancellation of contract fee, is at the delegated approver's discretion and such costs will be charged to the relevant cost centre.

4.11 All relevant mobile device details and call charges will be recorded in CQUniversity's Internal Billing System maintained by IaTD. All devices will be asset-tagged before being issued to employees.

4.12 Employees must return devices that are no longer required to IaTD so the service number can be cancelled, and the device reissued to another CQUniversity employee if suitable.

Supervisor access to absent employee email accounts and file storage

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

4.14 A request to arrange access to an absent employee's email or file storage must be made by the relevant Deputy/Pro/Associate Vice-Chancellor or Director/Dean to the People and Culture Directorate who will make appropriate arrangements with IaTD.

Using University-owned end user computing and mobile devices

4.15 The University issues end user computing devices such as desktops, laptops, tablets and mobile devices to employees for the primary purpose of delivering teaching, research and business operations on the University's behalf. The employee is responsible for the following:

a) ensuring data is not stored on local devices (hard drives) unless it is backed up/synchronised with a supported University backup service

b) ensuring devices are regularly connected to the University network for security and software updates.

4.16 Recommended practice for working with University data is to store it in the following places:

a) network drives

b) AARNet Cloudstor file sharing service

c) Microsoft OneDrive to sync files between CQUniversity's Office365 site and local devices

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

4.17 The following must be reported to TaSAC:

a) security breaches and risks

b) damage, hardware and software faults,

c) stolen or lost hardware items and

d) unwanted computing equipment or devices (for reuse or disposal).

Replacing an existing device

4.18 CQUniversity may replace a device if the relevant delegated approver is satisfied a request for replacement is justified or business or technology changes justify replacement.

Returning or retaining devices when employment ceases

4.19 On ceasing employment with CQUniversity, employees must return University-supplied devices and accessories (including power supplies, cases, mobile SIM cards if applicable) in good working order to IaTD. IaTD will arrange to reissue the device to another user or cancel the service.

4.20 If the returned device is not in good order, the cost of necessary repair or replacement may be deducted from outstanding benefits or entitlements available to the employee under their contract of employment.

4.21 If the device is not returned, the employee will be charged the cost of its replacement. In addition, the SIM card will be cancelled and the device locked, unless prior arrangements to retain the device have been made.

4.22 Departing employees may request approval by the delegated approver to retain the device's service number. IaTD will provide Transfer of Service Number Forms from the Service Provider; however, the departing employee is responsible for transferring the existing service number to a personal account. If the service number has not been transferred by the agreed transfer date, CQUniversity will cancel the service number.

Responsibility for mobile devices

4.23 Delegated approvers must ensure that a genuine business need or other benefit to CQUniversity exists before allocating or purchasing a mobile device, and that the device is appropriate for employee's role within CQUniversity.

4.24 Delegated approvers (or their nominated Divisional/Directorate representative) are responsible for monitoring expenses incurred on any service numbers to ensure expenses are within acceptable limits.

4.25 Employees are allocated a device, and recorded as its custodian, on the basis that they accept full responsibility for their proper use, care, maintenance and safe keeping. This includes responsibility for corporate mobile devices and their accessories, and for any activities associated with the device.

4.26 Employees are responsible for monitoring their own usage of the device including calls, data and other services to ensure they do not unnecessarily exceed their allotted plan. If the employee's carelessness is found to have contributed to the device's loss, the employee may be required to contribute to the replacement cost.

4.27 Any penalties or infringements for using a CQUniversity-owned mobile device whilst driving a CQUniversity or private vehicle is the employee's responsibility.

Using personal ICT devices

4.28 The University permits users to connect their own personal devices[1] to the University network.

4.29 All users of personal devices which connect via any means to University ICT facilities must ensure that the devices are secure and do not pose any threat to the network's operation.

4.30 Users of personal devices are required to adhere to this policy and procedure at all times when connected to any University-provided ICT facility (including connecting to the University network) and agree that:

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

[1] Using personally-owned devices at CQUniversity is sometimes referred to as BYOD, i.e. bring your own device.

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 are required to remove all university data and software from personal devices.

4.31 The following minimum requirements must be met before users connects any personal ICT devices to University ICT facilities:

a) to prevent unauthorised access, devices must be password protected using the features of the device and 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, as released by the manufacturer, and must be capable of connecting to the University enterprise wireless networks (e.g. Eduroam)

c) 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

d) 'Jailbroken' (Apple iOS and Android) devices are strictly forbidden from accessing the University network, as are devices with any unlicensed (pirated) operating systems.

4.32 The University may monitor use of its ICT facilities by connected personal ICT 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.

4.33 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 except in exceptional circumstances, such as excessive business requirements, 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).

Servers

4.34 All servers are to be located in an IaTD-managed datacentre or with an approved hosting provider. Employees must not create and/or operate servers or commission hosting services without IaTD's knowledge and endorsement.

Employees to lock computers

4.35 Employee workstations are configured to lock after a defined idle period; however, employees with access to sensitive or confidential information are required to manually lock their workstations before leaving them unattended to reduce the risk of unauthorised access (e.g. on a Microsoft Windows workstation use the windows symbol key + the 'L' key).

Monitoring use of CQUniversity resources

4.36 The University reserves the right to monitor (including recording and/or maintaining electronic logs) any and all aspects of its electronic information systems and devices (including mobile devices) to determine if a user is acting unlawfully or in violation of this policy and procedure.

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

University communication

4.38 The University uses the internet, email, portal technologies and other ICT facilities as official means of communication with staff and students. Email communication methods include, but are not limited to, email distribution, official employee mailing lists and the StaffNet intranet.

Email distribution lists

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

The official employee mailing list

4.40 The official employee mailing list official@lists.cqu.edu.au is the official means of distributing messages to all employees. All employees must maintain membership of this mailing list.

4.41 The Vice-Chancellor and President, Deputy Vice-Chancellors, Pro Vice-Chancellors and Heads of Directorates will be able to post to the list. Additional authorised users may be added with approval by the Vice-Chancellor and President or delegate, i.e. the Deputy Vice-Chancellor (International and Services).

4.42 Messages from all other employees will be moderated to ensure the messages are appropriate for the list and relevant to all employees.

StaffNet

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

Adult content

4.44 Adult content is blocked for all employees, students and visitors to CQUniversity.

4.45 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 (see consequences for breach of policy).

4.46 Application can be made to TaSAC for exemption and to be added to an exclusion group that allows access to adult content sites. Applications must include approval from the Ethics Committee and relevant supervisor. Those currently exempt are researchers, academics, teachers or students whose legitimate area of research or teaching involves adult-rated content.

Consequences for breach of policy

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

a) **CQUniversity employees**: a breach of this policy 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**: a breach of this policy may be treated as alleged student behavioural misconduct. Any disciplinary action will be managed in accordance with the Student Behavioural Misconduct Procedure or other relevant policy or procedure

c) **All other individuals, including visitors**: a breach of this policy will have their information and communication technology access rights revoked. If appropriate, further action may be taken in accordance with relevant CQUniversity policies and procedures or relevant legislation, including the *Central Queensland University Act 1998* (Qld).

5 RESPONSIBILITIES

Compliance, monitoring and review

5.1 The Senior Deputy Vice-Chancellor (International and Services) is responsible for monitoring, reviewing and ensuring compliance with this policy and procedure.

Reporting

5.2 No additional reporting is required.

Records management

5.3 Staff must maintain all records relevant to administering this policy and procedure in a recognised University recordkeeping system.

6 DEFINITIONS

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

Terms and definitions

Adult content: any media or photographs showing erotic or sexual behaviour in a way designed to cause sexual arousal, also known as pornography.

Delegated approver: an employee with authority to make decisions regarding an individual's use of a University-funded mobile device. Delegated approvers are as follows:

Category of individual	Delegated Approver
Senior executive	Vice-Chancellor and President
Academic / teacher employee	Dean/Provost
Professional employee	Deputy or Pro Vice-Chancellor/ /Director/Dean

Devices or CQUniversity-owned devices: means 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 CQUniversity has purchased and provided to individuals to use for official University business.

Employee: any person employed by CQUniversity on a permanent, fixed-term, casual basis or subsidiary companies.

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

Jailbroken: refers to 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.

Service number: means the mobile number attached to a mobile service, whether for mobile voice or data services, to which the service costs will be charged.

SIM (subscriber identity module): means a card that enables a mobile device to connect to the service provider's network.

Standard services: include voice calls, voicemail, SMS, MMS and data plans.

Visitor: any person who is not a CQUniversity student or employee.

7 RELATED LEGISLATION AND DOCUMENTS

Central Queensland University Act 1998 (Qld)

Central Queensland University Enterprise Agreement

Code of Conduct

Procurement Policy and Procedure (FMPM)

Research Data Management Policy and Procedure

Student Behavioural Misconduct Procedure

Use of ICT Services, Facilities and Devices Policy (IS38)

8 FEEDBACK

8.1 University staff and students may provide feedback about this document by emailing policy@cqu.edu.au.

9 APPROVAL AND REVIEW DETAILS

Approval and Review	**Details**
Approval Authority	Vice-Chancellor and President
Advisory Committee to Approval Authority	Vice-Chancellor's Advisory Committee
Administrator	Senior Deputy Vice-Chancellor (International and Services)
Next Review Date	7/08/2021

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; Administrator Approved – Acting Senior Deputy Vice-Chancellor (International and Services) 16/10/2018.
Notes	This document consolidates and replaces the Acceptable Use of Information and Communications Technology Facilities and Devices Policy and Procedure and the Mobile Device Principles (7/08/2018).