Information and Communications Technology (ICT) Appropriate Use Procedures

1. STRATEGIC PLAN THEME AND COMPLIANCE OBLIGATION SUPPORTED

Information Security & Information and Communication Technology (ICT) Appropriate Use Policy

Strategic Plan Theme: Sustainable Futures

2. PROCEDURAL DETAILS

Users are provided access to Information Communications Technology (ICT) Assets to support the University's core business activities. To ensure appropriate and responsible use of ICT Assets, the following procedural statements have been defined.

2.1. Approval and Acknowledgment

2.1.1. Users will use ICT Assets for authorised purposes, such as official University business or University approved research and development, and limited Personal Use.

2.1.2. Approval to use ICT Assets will be obtained from the User's line manager or the ICT Asset Owner (or their authorised representative) as applicable.

2.1.3. Access to ICT Assets will be provided in adherence to the Principle of Least Privilege, so that Users will only be provided with the minimum privileges and access rights required to perform their job functions.

2.2. Appropriate Use of ICT Assets

2.2.1. Users will protect ICT Assets from unauthorised access or disclosure by not disclosing to others nor leaving unprotected, their Account Credentials and adhering to handling requirements as determined by the ICT Asset's information security classification.

2.2.2. Users will notify CITS if an ICT Asset malfunctions or is damaged, stolen or lost.

2.2.3. Users will take all Reasonable Care when downloading, accessing or executing files, accessing websites or links, on or from the internet.

2.2.4. For the purposes of testing and improving security controls or system auditing, ICT Asset Owners, as authorised by an Executive Manager, the Chief Information Officer (CIO), or their authorised representative, may be given permission to access User's University IT account, digital information or Account Credentials.

2.2.5. Users will store University information on University approved storage, i.e. CITS managed file services, commensurate with the appropriate information security classification.

2.2.6. If requested, users will be able to demonstrate (via appropriate University identification, email or similar) that they are permitted to use ICT Assets.

2.3. Limited personal use

2.3.1. The University allows limited Personal Use of the internet and electronic communications facilities. Such use will comply with the requirements outlined in these procedures and in the related information security policies. Personal Use may be monitored – refer Section 2.6.

2.3.2. Users will consider the following conditions for Personal Use:

a. The University is not impacted financially.

b. University business objectives are not unduly impacted.

c. Personal Use does not breach any University Statutes, Rules, policies or procedures.

2.4. Inappropriate Use of ICT Assets

2.4.1. Users will not:

a. Email, publish, or reveal to others, University Account Credentials.

b. Download and/or access files or click on any links to websites without exercising Reasonable Care and considering whether the content may adversely affect ICT Assets.

c. Attempt to access another user's digital information without authorisation from an Executive Manager, the CIO, or their authorised representative for the business or purpose of the University.

d. Carry out activities that violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations.

e. Upload, download, install or distribute unlicensed or inappropriately licensed software.

f. Attempt to subvert IT technical configurations, such as Security Measures in any way, possess any prohibited tools that may be used to subvert security measures, nor use a false identity, when using ICT Assets, unless authorised by an Executive Manager, the CIO, or their authorised representative and for the business or purpose of the University.

g. Interfere with or attempt to interfere with the investigation of a breach of University policy by:

    - Electronic means – concealing, modifying or erasing the evidence of a breach.
    - Physical means – disposing of or altering hardcopy records.
    - Social means – disseminating false statements.

h. Obstruct others in the lawful use of, or attempt to interfere with the lawful operation of ICT Assets.

i. Access, publish, transmit, or cause to be transmitted, through ICT Assets or over the University network any information of an obscene, profane or otherwise harmful material likely to be sexually offensive to an ordinary prudent and rational person, except where done for the business or purpose of the University. Clear examples of such material include, but are not limited to materials that:

    - Contain sexually explicit images or descriptions.
    - Advocate illegal activity.
    - Advocate intolerance or hatred for others.
    - Are bullying or harassing in any way.
    - Breach state and / or federal law.

j. Use, nor direct, encourage, engage with or knowingly allow others to use, any ICT Assets to devise or execute any scheme to defraud or to obtain money, property, services, or other things of value by false pretences, promises, or representations.

k. Forward emails containing non-public University information to personal email accounts by either auto-forwarding or manual means, unless authorised by an Executive Manager, the CIO, or their authorised representative for the business or purpose of the University.

l. Wilfully waste ICT Assets by downloading or sending large amounts of material (e.g. spam emails) that are not for the business or purpose of the University.

m. Use University ICT Assets for commercial purposes nor publish or circulate information about other organisations via ICT Assets, except where these activities are for the business or purpose of the University.

2.4.2. The following actions are not permitted with respect to the technical use of ICT Assets:

a. Destroy, alter, dismantle, prevent rightful access to or otherwise interfere with the integrity of ICT Assets.

b. Access, copy, alter or destroy information, electronic mail, data, software or other files without authorisation by the following roles:
    - Executive Manager, the CIO, or their authorised representative for matters relating to access.
    - Associate Director Curtin Information Management and Archives for matters of records management.
    - Information Asset Owner for all other matters.

c. Seek, nor direct, encourage, engage with or knowingly allow others to seek to gain unauthorised access to ICT Assets.

d. Severely degrade or disrupt equipment or system performance.

e. Export software, technical information, encryption software or technology, in violation of international or regional export control laws.

f. Knowingly introduce inappropriate software into the network or server environment including but not limited to, incorrectly licensed software; software which has been modified to disrupt or avoid valid licensing mechanism such as ‘cracks’ or ‘cracked software’; and introducing software which may adversely impact the security of an ICT Asset such as malware including viruses, worms, Trojan horses or e-mail bombs.

g. Effect security breaches or disruptions of network communication. Security breaches include, but are not limited to:
    - Accessing data to which the user is not an intended recipient.
    - Logging into a server or account that the user is not expressly authorised to access.
    - For the purposes of this section, "disruption" includes, but is not limited to:
        - Network sniffing – capturing network data to aid malicious activities.
        - Packet spoofing – creating a false network identity to hide the source.
        - Denial of service – causing ICT Assets to be unavailable to Users.
        - Forged network routing information for malicious purposes.

h. Execute any form of network monitoring which will intercept data not intended for the user’s host or network security scanning, unless authorised by an Executive Manager, the CIO, or their authorised representative for the business or purpose of the University.

i. Circumvent user authentication or security of any host, network or account.

j. Use any program/script/command or send messages of any kind, with the intent to interfere with, or disable a user's terminal session via any means.

2.4.3. Inappropriate behaviour with respect to the use of ICT Assets includes, but is not limited to the following actions:

a. Breach the University Privacy Statement impacting the protection of personal information.

b. Participate in gambling activities such as may be provided by casino and internet-based gambling sites.

c. Misrepresent him/herself or the University.

d. Make fraudulent offers of products, items, or services originating from any University account.

e. Operate a business using University ICT Assets.

f. Violate any State, Commonwealth or international laws.

2.5. Personal Devices

2.5.1. Users will ensure appropriate security controls are applied to non-University devices, including but not limited to:

a. Installation and continued operation of Curtin software to control or monitor the non-University device.

b. Installation and continued operation of security protective software including anti-malware software, device firewall policies and where available, remote wiping or erasure software.

c. Use of appropriately configured computer account passwords for the security classification of the data accessible on or from the device.

2.5.2. Users will limit storing University information on personal devices.

2.5.3. Where a staff member terminates a working relationship with the University, all University data from the device will be removed and deleted securely.

2.6. Monitoring and Privacy

2.6.1. Users will be responsible to immediately report potential and actual breaches of the Information Security & ICT Appropriate Use Policy or this procedure to their line manager and the CITS Service Centre to support effective and efficient monitoring.

2.6.2. The University will monitor the access and use of its ICT Assets, including the content of all electronic communications for, but not limited to the following purposes:

a. Where it is required by law.

b. To enable or facilitate investigations or enquiries into alleged misconduct, violations of law, University statutes, rules, policies or procedures or grievances.

c. To protect the security of ICT Assets.

d. To satisfy the requirements of the Freedom of Information Act 1992 (WA).

e. To protect personal information as per the University's Privacy Policy.

2.6.3. Initial inspection of another User's digital information is strictly limited to the person requesting access or the nominated person, only once it has been authorised and justified in writing by any of the following:

a. Executive Manager;

b. Director, People and Culture;

c. Chief Information Officer;

d. Academic Registrar;

e. Director, Integrity and Standards Unit;

f. Authorised representatives of the positions a. to e. above;

g. An officer acting under the Freedom of Information Act 1992 (WA); or

h. The User subject to inspection of digital information, providing they are a current employee.

2.6.4. Where it is believed the circumstances may lead to investigation of or enquiry into a potential breach of statutes, rules, University policy or procedures, the requester will consult with the Director, People and Culture, Associate Director Curtin Information Management and Archives or Academic Registrar (as appropriate).

2.6.5. The University will filter internet content. The CIO or their representative, may exempt Users from content filtering based on business activities, supported by approval from their line manager(s) or supervisor.

2.6.6. All Reasonable Care is taken to protect Users privacy. However, the content of personal electronic communications, documents and data stored on ICT Assets may be inspected with the authorisation from the positions listed in Section 2.6.3 where required based on Section 2.6.2.

2.7. Consequences of a Breach

2.7.1. The University will suspend a User's access to ICT Assets where there are reasonable grounds to suspect that a User has breached these procedures or any relevant legislation or contract(s).

2.7.2. The University may undertake any lawful action (including disconnecting devices from the network or deactivating sub-networks) to protect and ensure integrity of ICT Assets, as well as University information.

2.7.3. The University may restrict activities to maintain the service quality or availability of ICT Assets.

2.7.4. Misuse of ICT Assets will be dealt with in accordance with the relevant disciplinary processes, and in the event of criminal conduct, may be referred to relevant law enforcement or government oversight agencies.

3. RESPONSIBILITIES

In addition to any responsibilities set out in Section 2, the following responsibilities are defined.

3.1. Executive Manager

Is responsible for:

a. Overseeing, supporting and communicating this procedure.

b. Providing authority to authorised staff members to monitor and audit the use of ICT Assets.

3.2. Chief Information Officer (CIO)

Is responsible for:

a. Overseeing the implementation of adequate controls to comply with this procedure.

b. Providing authority to authorised staff members to monitor and audit the use of ICT Assets.

c. Approving exceptions to this procedure.

d. Providing ICT Assets that support enterprise functions.

3.3. Chief Information Security Officer

Is responsible for:

a. Establishing adequate controls to comply with this procedure.

b. Establishing an ongoing information security awareness campaign intended to raise user security awareness when using the University's ICT Assets.

3.4. Director, People and Culture; Director, Integrity and Standards Unit; Academic Registrar

Is responsible for overseeing and providing authority to authorised staff members to monitor and audit the use of ICT Assets.

3.5. Line Managers and Supervisors

Are responsible for:

a. Advising the University community of their obligations with respect to this procedure.

b. Promoting this procedure.

3.6. University Community

Are responsible for:

a. The ethical and efficient use of ICT Assets as prescribed in this procedure.

b. Reporting security incidents and any identified weaknesses.

4. SCOPE OF PROCEDURES

These procedures apply to the University Community in all Curtin University campuses, and where not already covered, to ICT assets owned, managed, controlled and leased by the University, or as applicable by commercial or legal arrangement.

5. DEFINITIONS

(Note: Commonly defined terms are in the *Curtin Common Definitions*. Any defined terms below are specific to this document)

Account Credentials
User account credentials for ICT Assets include, but are not limited to:

- Usernames.
- Passwords and passphrases.
- Security tokens (such as smartphones to provide two-factor authentication).

Authorised Staff Member
A University staff member authorised by the University to request University identification from a member of the University community. An authorised staff member status will be displayed on their University identification.

Chief Information Officer (CIO)
As defined by University role, or in the alternative, the contracted Head of IT in offshore locations.

ICT Assets
Any information, communications technology or audio-visual service, equipment or facility owned leased or contracted by the University that hosts, stores, transmits or presents digital information for the business and purpose of the University. This may include, but is not limited to:

- Software applications.
- Physical and virtual hardware.
- Email, messaging and collaboration applications.
- Any outsourced cloud or third-party services.
- Interconnected devices and embedded systems that can communicate or interact with other ICT Assets.
- Audio-visual systems and devices.
- Telephony, videoconferencing and web conferencing systems, services and applications.

ICT Asset Owner
An ICT Asset Owner is an authorised representative of the University who is the accountable decision maker for ICT Assets. For example:

- The Chief Financial Officer is the ICT Asset Owner of the payroll system.
- The Chief Information Officer is the ICT Asset Owner of CITS ICT infrastructure.

Internet of Things (IoT)
IoT is a collection of physical and virtual devices connected on the backbone of other, already established, communications networks. For example, *things* such as automated lighting or swipe card locks to buildings, which can be uniquely identified on a network.

Personal Device
ICT equipment or devices not provided to Users by the University that are used to access ICT Assets. Typically, these will be mobile phones, tablets and laptops. Also referred to as 'Bring Your Own Device' – BYOD.

Personal Use
Incidental use of ICT Assets that is not for the business or purpose of the University. For example, personal emails, online banking and social networking.

Reasonable Care
The degree of caution or concern an ordinary prudent and rational person would use in the circumstances. For example, if a file, link or website is not known to be safe then, it will be expected that the User will not download, access or execute a file on or from the internet.

Security Measures
Also referred to as personnel, technical or process security controls used to ensure effective operations of the University by managing the confidentiality, integrity and availability of ICT Assets.

Two-Factor Authentication
A user is required to provide at least two forms of authentication information as follows:

- "Something you know" – Password, passphrase.
- "Something you have" – Security token, swipe card.
- "Something you are" – Fingerprint, iris or retinal scan.

Users
Any member of the University Community who uses or accesses an ICT Asset.

6. RELATED DOCUMENTS/LINKS/FORMS

Statute No. 10 – Student Discipline

General Misconduct Rules

Employee Code of Conduct

Student Conduct

Information Security Classification Policy

Information Management Policy

Compliance Procedures

Policy Compliance Officer	Mark Calleja, Manager, IT Planning, Governance and Executive Support
Policy Manager	Chief Operating Officer
Approval Authority	Chief Operating Officer
Review Date	1st April 2022

REVISION HISTORY

Version	Approved/ Amended/ Rescinded	Date	Committee / Board / Executive Manager	Approval / Resolution Number	Key Changes & Notes
New	Approved	02/10/2018	Chief Operating Officer	EM1821	Unconditional