Information and Communications Technology (ICT) Appropriate Use Procedures

1. COMPLIANCE OBLIGATION SUPPORTED

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

2. PROCEDURAL DETAILS

The University community is provided access to Information Communications Technology (ICT) assets to support the University's activities. To ensure appropriate and responsible use of these ICT assets, the following procedural statements have been defined.

2.1. Approval and Acknowledgment

2.1.1. Approval to use ICT assets will be obtained from the user's line manager or their delegate as applicable.

2.1.2. Access to ICT assets will be provided in adherence to the principle of least privilege, so that ICT asset users will only be provided with the minimum privileges and access rights required to perform their functions.

2.1.3. All staff and contractors must complete mandatory cyber security training within the University's set timeframes.

2.1.4. Anyone in the University Community must report any suspected cyber security threat or incident immediately upon discovery.

2.2. Appropriate Use of ICT assets

2.2.1. ICT asset users will take all reasonable steps to protect ICT assets from unauthorised access by protecting and not disclosing their account credentials and by adhering to all cyber security requirements.

2.2.2. ICT asset users will notify Digital and Technology Solutions (DTS) if an ICT asset malfunctions or is damaged, stolen or lost.

2.2.3. ICT asset 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), the Chief Information Security Officer (CISO), or their delegate, may be given permission to access User's University ICT asset or account credentials.

2.2.5. ICT asset users will store University Information on University supported storage, i.e. Digital and Technology Solutions (DTS) managed services, commensurate with the appropriate information security classification as per the Information Management policy and procedures.

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

2.2.7. The University staff and contractors will take all reasonable steps to ensure that third-party providers handling the University's ICT assets will follow the University's cyber security requirements during procurement and as agreed by contract or other relevant agreements as applicable.

2.2.8. Anyone accessing the University's ICT assets must adhere to the University's values, applicable laws, policies, and procedures.

2.2.9. If provided with access to ICT assets through a University account, members must not disclose account details unless:

a) It is for an authorised purpose.

b) Approved by the Chief Information Officer (CIO), Chief Information Security Officer (CISO) or their delegate(s).

c) Required by Law.

2.3. **Inappropriate Use of ICT assets**

2.3.1. ICT asset users will **not**:

a) Email, publish, or reveal or disclose their 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 delegate for the business or purpose of the University.

d) Carry out activities that violate the rights of any person or company protected by any relevant laws or regulations.

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

f) Attempt to subvert IT technical configurations or 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, the CISO, or their delegate 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 any means, to include:

- Electronic means – concealing, withholding, modifying, deleting, or erasing the evidence of a breach.
- Physical means – disposing of, modifying, withholding, or altering hardcopy records.
- Social means – disseminating false or otherwise vexatious 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 offensive to a reasonable person, except where done for the business or purpose of the University and with prior approval from the CIO or an Executive Manager. Clear examples of such material include, but are not limited to materials that:

- Contain sexually explicit or indecent images or descriptions.
- Advocate illegal activity.
- Advocate intolerance or hatred for others.
- Are bullying or harassing in any way.
- Advocate or solicit violence, cruelty, or harm.
- 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 any external email accounts by either auto-forwarding or manual means, unless authorised by an Executive Manager, the CIO, or their delegate 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.

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

a) Destroying, altering, dismantling, or preventing rightful access to or otherwise interfere with the integrity of ICT assets.

b) Seeking, nor directing, encouraging, engaging with, or knowingly allow others to seek to gain unauthorised access to ICT assets.

c) Severely degrading or disrupting equipment or system performance.

d) Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws.

e) Knowingly introducing 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’; or knowingly introducing software which may adversely impact the security of an ICT asset such as malware including viruses, worms and Trojan horses.

f) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to:

i. Accessing data to which the user is not an intended recipient.

ii. Logging into a server or account that the user is not expressly authorised to access.

iii. For the purposes of this section, "disruption" includes, but is not limited to:

a) Network sniffing – capturing network data to aid malicious activities.

b) Packet spoofing – creating a false network identity to hide the source.

c) Denial of service – causing ICT assets to be unavailable to ICT asset users.

d) Forged network routing information for malicious purposes.

g) Executing 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, the CISO, or their delegate for the business or purpose of the University.

h) Circumventing user authentication or security of any host, network or account unless authorised by an Executive Manager, the CIO, the CISO, or their delegate for the business or purpose of the University. Using any program/script/command or send messages of any kind, with the intent to wilfully interfere with, disrupt or disable a user's terminal session via any means where there is no operational or business need to do so.

i) Breaching the University Privacy Policy or any action which will impact the protection of personal information.

j) Participating in gambling activities such as may be provided by casino and internet-based gambling sites.

k) Misrepresenting themselves or the University.

l) Making fraudulent offers of products, items, or services originating from any University account.

m) Operating a business using University ICT assets.

n) Violating any State, Commonwealth, or international laws.

2.4. **Limited Incidental Personal Use**

2.4.1. The University allows limited incidental personal use of the internet and electronic communications facilities. Such use will comply with the requirements outlined in these procedures and in the related Cyber security policies. Personal use may be monitored – refer Section 2.5.

2.4.2. ICT asset users will adhere to the following conditions for Limited Incidental Personal Use:

a) The University is not impacted financially.

b) University business objectives, duties, and staff responsibilities are not unduly impacted.

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

2.5. **Personal Devices**

2.5.1. ICT asset users will avoid storing University information on personal devices.

2.5.2. ICT asset users will maintain relevant operating system and other software updates and security patches.

2.5.3. ICT asset users will ensure appropriate security controls are applied to non-University devices. The University reserves the right to prevent access to University technology and resources where this does not occur, and compliance will be subject to monitoring and inspection.

2.5.4. Where an ICT asset user terminates a working relationship with the University, all University data from the device must be removed from the device unless authorised by University.

2.6. **Incident Reporting, Monitoring and Privacy**

2.6.1. To support effective and efficient monitoring, ICT asset users will be responsible to immediately report:

a) potential and actual breaches of the *Cyber Security and Information and Communication Technology (ICT) Inappropriate Use Policy*;

b) potential and actual breaches of these Procedures;

c) Information Breaches; and

d) Privacy Incidents

to their line manager and the Digital and Technology Solutions (DTS) Service Desk in accordance with the Information Breach Policy and Information Breach Procedures.

2.6.2. All reported threats and incidents will be reviewed, and as appropriate, reported to the relevant government agency and cyber security incidents involving personal or sensitive information must be reported per the Information Breach Procedures.

2.6.3. The University reserves the right to monitor and review the use of ICT assets.

2.6.4. The University will investigate unauthorised use of the University's ICT assets.

2.6.5. The University may limit, disable, or remove access to ICT assets if there is an actual or perceived threat to the University's operations or an unacceptable cyber risk.

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

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, 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 and sensitive personal information in accordance with the University's Privacy Policy and Privacy Procedures.

2.6.7. 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) Chief People Officer;

c) Chief Information Officer;

d) Academic Registrar;

e) Director Risk, Compliance & Audit;

f) Delegates of the positions above;

g) An officer acting under the Privacy and Responsible Information Sharing Act (WA) 2024;

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

i) The individual who is the subject of the digital information, providing the request is made in accordance with the Freedom of Information Act 1992 (WA).

2.6.8. Where it is believed, that 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 Chief People Officer, Chief Legal Officer, Director, Data and Information Governance, Director, Risk, Compliance & Audit, Chief Information Officer, Associate Director Curtin Information Management and Archives or Academic Registrar as appropriate.

2.6.9. The University will filter internet content based on the risk appetite of the University. The CIO or their representative, may exempt ICT asset users from content filtering based on business activities, supported by approval from an Executive Manager.

2.6.10. All reasonable care is taken to protect ICT asset 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

2.6.11. All ICT assets will be managed and tracked through relevant systems and processes.

2.7. **Consequences of a Breach**

2.7.1. The University may 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, and quarantining and deleting files) to protect and ensure the integrity of ICT assets and information assets.

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

Responsibilities are as set out in Section 2. In addition:

3.1. **Executive Manager**

Is responsible for:

a) Overseeing, supporting, and communicating these Procedures.

b) Authorising staff members to monitor and audit the use of ICT Assets.

3.2. **Chief Information Officer (CIO)**

Is responsible for:

a) Overseeing the management and mitigation of risks to ICT assets to comply with these Procedures.

b) Allocating sufficient resources and support for managing cyber security risks.

c) Authorising staff members to monitor and audit the use of ICT Assets.

d) Approving exceptions to these Procedures.

3.3. **Chief Information Security Officer (CISO)**

Is responsible for:

a) Facilitating cyber security risk management and compliance practices.

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

c) Liaising with Government agencies on cyber security matters.

3.4. **Line Managers**

Are responsible for:

a) Advising the University community of their obligations with respect to these Procedures.

b) Supporting and participating in any cyber security reviews conducted by the Chief Information Security Officer.

c) Promoting these Procedures.

3.5. **University Community**

Is responsible for:

a) The ethical and efficient use of ICT assets as prescribed in these Procedures.

b) Reporting security threats or incidents and any identified weaknesses.

4. SCOPE OF PROCEDURES

These Procedures apply to all members of the University community (which includes Council members, students, employees, University Associates, Curtin controlled entities, and all persons participating in University business or activities, including whether as a visitor, adjunct appointee, service provider, or contractor) in any location or campus within Australia or offshore.

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).

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 purposes 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 the accountable decision maker for ICT Assets. For example:

- The Chief Financial Officer is the ICT asset Owner of the financial system.
- The Chief Information Officer is the ICT asset Owner of Digital and Technology Solutions (DTS) ICT infrastructure.

Limited Incidental Personal Use
Infrequent or occasional 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.

Technology Device
Any Curtin owned or managed hardware used for business activities. Examples include desktop and laptop computers, mobile phones, tablets, audio-visual equipment such as projectors and televisions, desktop phones, network equipment, and physical server infrastructure.

ICT asset users
Any member of the University Community who uses or accesses an ICT asset.

6. SCHEDULES

Nil

RELATED DOCUMENTS/LINKS/FORMS

Internal

- Code of Conduct
- Curtin Information Statement
- *Cyber Security Procedures*
- Reporting Information Security Incidents
- IT Security Standards
- *Information Breach Policy* and *Procedures*
- *Information Management Policy and Procedures*
- *Privacy Policy* and *Procedures*

External

- *Privacy and Responsible Information Sharing Act (WA) 2024*
- *Criminal Code Act Compilation Act 1913 (WA)*
- *Australian Privacy Principles*
- *Electronic Transactions Act 2011 (WA)*
- *Evidence Act 1906 (WA)*
- *Freedom of Information Act 1992 (WA)*
- *Privacy Act 1988 (Cth)*
- *State Records Act 2000 (WA)*
- *WA Government Information Classification Policy*
- *Privacy and Responsible Information Sharing Act (WA)*
- *Security of Critical Infrastructure Act 2018 (Cth)*
- *2024 WA Government Cyber Security Policy*
- *Cyber Security Act 2024 (Cth)*
- *Higher Education Standards Framework (HESF)*: Standards 2.1.2 & 7.3.3

Policy Compliance Officer	Anita Mathews, Cyber Security Assurance Lead
Policy Manager	Chief Operating Officer
Approval Authority	Chief Operating Officer
Review Date	1st April 2030

REVISION HISTORY (*filled out by Risk, Compliance and Audit*)

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
	Approved	24/03/2022	Chief Operating Officer	EM2206	
	Approved	27/10/2026	Chief Operating Officer	EM2618	