Use of ICT Services, Facilities and Infrastructure Procedure

Version 3 – Approved 7 December 2023

Contents

Purpose

This procedure describes who can use the University's Information and Communication Technology (ICT) services, facilities and infrastructure, the conditions of use and how use is managed.

Applicable governance instruments

Instrument	Section	Principles
Data and Information Governance Policy	3 Information, communication and technology services and facilities use	3.1 - 3.6
Intellectual Property Policy	5 Copyright	5.1 - 5.2
Behaviour Policy	6 Governance and Accountability	6.4

Procedure

1. Introduction

ICT services, facilities and infrastructure are provided by the University to support research, teaching, learning, and University operational activities and include the following:

- Services – such as installation of software, device updates, configuration of devices, ICT support.
- Authorised users are defined as university students, staff, and researchers.

- Infrastructure and Systems – including computers and telephones, computing laboratories and video conferencing rooms, networks, software, owned or leased by the University.

The conditions of use described in this procedure apply to:

- all University Community members
- all ICT services provided by the University
- all ICT facilities and infrastructure owned or leased by the University
- any privately owned device that connect to the University infrastructure.

2. Authorised Users and Access

2.1. The University's ICT services, facilities and infrastructure can only be used by authorised users. Authorised user accounts are granted in accordance with the *Cyber Security Controls Procedur*e.

3. General Conditions of Use

3.1. The University's ICT services, facilities and infrastructure must be used in a manner that supports the University's reputation, mission and values and:

a. may only be used for University business purposes including learning, teaching, research, professional development and operational activities, and

b. must not be used for non-University commercial purposes or personal financial gain.

3.2. All use must be legal, ethical and consistent with the University's *Data and Information Governance Policy*, *Behaviour Policy* and *Behaviour Procedure.* It is the responsibility of the authorised user to comply with all University policies and procedures and applicable Australian and State Government legislation.

4. Software on ICT Systems

4.1. University ICT systems must be configured to an IT Services Standard Operating Environment build. All exceptions must be approved by the Chief Information Officer.

4.2. No additional software is to be installed onto University ICT systems, or configuration changes made, unless approved by the Chief Information Officer or nominee.

4.3. Use of all software must comply with the software providers End User Licences Agreement (EULA).

5. Internet and Online Services

5.1. The University provides authorised users access to the internet and University online services.

5.2. The University may restrict or block access to services, IP addresses, locations, or internet sites if they are assessed as posing an unacceptable risk to the University's reputation, systems or infrastructure.

5.3. All access restrictions or removals will be approved by the Chief Information Officer or nominee.

5.4. Where possible, access to services or websites used for research, learning and teaching or University business purposes will not be restricted.

6. Use of Copyright Materials on University ICT systems

6.1. The University's ICT Services, Facilities, and Infrastructure may not be used to download, copy,

store, transfer or redistribute materials (for example movies, music etc) without the permission of the copyright owner.

6.2. The University holds licences which permit certain copyrighted material to be copied, stored and communicated for teaching or research purposes. Staff and students must comply with all licence conditions relating to the use of such material.

6.3. Further information regarding the use of copyrighted materials for teaching or research purposes is available on the University's Copyright website. Advice can also be sought from the University's Copyright Officer: utas.copyright@utas.edu.au

6.4. Any material which infringes or is alleged to infringe copyright will be removed from any ICT Services, Facilities, and Infrastructure in accordance with the University's *Copyright Complaints and Takedown Procedure*. Where a service or website, external to the University is identified as a source of infringing material, the University will block access and remove content from the service or website.

7. Connection of Privately Owned Devices

7.1. Privately owned devices are not to be connected to the University's wired network ICT infrastructure without prior approval of the Chief Information Officer or nominee.

7.2. Privately owned devices may only access ICT services that are provided for the purposes of learning, teaching and research, or where the data custodian authorises access or where there is a self-service capability.

7.3. The University is not responsible for the management or maintenance of privately owned devices, or for loss or damage to a personal device.

8. Modifications to ICT Services, Facilities and Infrastructure

8.1. All network modifications must be approved by the Chief Information Officer or nominee. Network modifications may only be carried out by authorised personnel. Network modifications include, but are not limited to:

a. disconnecting computers from the University network

b. connecting unregistered devices of any type

c. connecting hubs and switches

d. tampering or attempting to modify any network device.

8.2. Unless part of an approved network modification, the installation of a port splitter or any network communication device that supports multiple simultaneous connections to a single network port or third-party network(s) is prohibited.

9. Monitoring Use

9.1. All use of the University's ICT services, facilities and infrastructure are monitored, and usage information collected in accordance with the *Cyber Security Controls Procedure*.

9.2. If any illegal or unauthorised activity is detected, the University will take appropriate action to stop the activity and refer the matter to appropriate internal or external authorities.

10. Access to the email and electronic data of another authorised user

10.1. Requests from authorised users to access the email or electronic data of another current or former authorised user will generally be denied, unless a compelling justification is provided and approved by either the current or former authorised user or General Counsel/Deputy General Counsel.

10.2. A request to General Counsel or Deputy General Counsel must:

- detail the type and nature of the information being requested,
- provide a justification for the access to the information, and
- include the written consent of the other current or former University Community member. If the consent of the individual has not been obtained, the request must include written permission from the relevant head of college/division, or other written authorisation, such as a court order or law enforcement request.

10.3. If a request is approved, IT Services will access and provide the approved information to the requestor. The requestor will not be granted global access to all of the University Community Member's email or electronic data.

10.4. The University uses and discloses personal information in accordance with relevant privacy and other legislation, and the University's *Data and Information Governance Policy* and Privacy Statements.

11. Access by former authorised user to email and electronic data

11.1. Once an account has been disabled at the offboarding of an authorised user, requests for retrieval of data will generally be denied, unless a compelling justification is provided and approved by the Associate Director Cyber Security.

Related procedures

Copyright Complaints and Takedown Procedure

Cyber Security Controls Procedure

Behaviour Procedure

Versions

Version	Action	Approval Authority	Responsible Officer/s	Approval Date
1	Approved	Chief Operating Officer	Chief Information Officer	30 November 2021
2	Approved	Chief Operating Officer	Chief Information Officer	7 December 2022
3	Approved	Deputy Vice- Chancellor (Student Services and Operations)	Chief Information Officer	7 December 2023