

Use of ICT Services, Facilities and Infrastructure Procedure

Version 2 – Approved 7 December 2022

Contents

Purpose.....	1
Applicable governance instruments.....	1
Procedure	1
1. Introduction	1
2. Authorised Users and Access	2
3. General Conditions of Use	2
4. Software on ICT Systems.....	2
5. Internet and Online Services.....	2
6. Use of Copyright Materials on University ICT systems	2
7. Connection of Privately Owned Devices	3
8. Modifications to ICT Services, Facilities and Infrastructure.....	3
9. Monitoring Use	4
10. Access to the email and electronic data of another University Community member	4
Related procedures	4
Versions	4

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
<i>Data and Information Governance Policy</i>	3 Information, communication and technology services and facilities use	3.1 - 3.6
<i>Intellectual Property Policy</i>	5 Copyright	5.1 - 5.2
<i>Behaviour Policy</i>	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.

- 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 Procedure*.

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 may only be used for:
- a. University business purposes including teaching, learning, research, personal or professional development and operational activities.
 - b. Limited appropriate personal use.
- They must not be used for commercial purposes or 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.
- 4.3. Use of all software must comply with the 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 or internet sites if they are assessed as introducing risk to the University's reputation, systems or infrastructure.
- 5.3. All access restrictions or removals will be approved by the Chief Information Officer.
- 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

Version 2 – Approved 7 December 2022

Definitions and acronyms can be found at: <https://www.utas.edu.au/policy/policy-definitions>

Related policy and procedures can be found at: <https://www.utas.edu.au/policy>

- 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: <http://www.utas.edu.au/copyright/>. Advice can also be sought from the University's Copyright Officer: utas.copyright@utas.edu.au
- 6.4. Authorised users may, purchase materials through online distributors using University ICT Services, facilities and infrastructure. These materials can be stored on University devices in accordance with the licence conditions under which they were purchased. It is the responsibility of the authorised user to ensure they manage the copyright materials in accordance with licencing conditions.
- 6.5. Authorised users may use University devices for streaming online content within the licensing conditions of the service, but may not store or distribute such materials using University ICT facilities and infrastructure. Private media libraries must not be stored on University owned devices.
- 6.6. 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.
- 7.2. Privately owned devices may only access ICT services where the data custodian authorises the connection, or the ICT Service or data store provides a self-service interface for the user.
- 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. 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
 - c. connecting hubs and switches.
- 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 University Community member

- 10.1. Requests from University Community members to access the email or electronic data of another current or former University Community member will generally be denied, unless a compelling justification is provided.
- 10.2. In the event that a University Community member requires access to the email or electronic data (including personal information) of another current or former University Community member, a request for access must be made to General Counsel or Deputy General Counsel.
- 10.3. 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.
- 10.4. 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.
- 10.5. 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.

Related procedures

Copyright Complaints and Takedown 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

Version 2 – Approved 7 December 2022

Definitions and acronyms can be found at: <https://www.utas.edu.au/policy/policy-definitions>

Related policy and procedures can be found at: <https://www.utas.edu.au/policy>