ICT Services and Facilities Use Policy

ICTP 3.1

Relevant UTAS Ordinance, Rule and/or GLP No.	Ordinance 9 – Student Discipline
Relevant State/Federal Govt. Legislation	Broadcasting Services Act 1992 Copyright Act 1964 Crimes Act 1914 Personal Information Protection Act 2004 (Tas) Telecommunications Act 1997
Commencement Date	June 2010
Review Date	Review 1 – June 2011 Review 2 – June 2014

POLICY STATEMENT

1 Intent

To ensure the appropriate use of the University's Information and Communication Technology (ICT) Services and define the responsibilities of users of the University's ICT Services and Infrastructure.

2 Scope

This policy applies to all University of Tasmania staff, students and associates.

3 Objective(s)

The objective of this Policy, and associated procedures and standards are to define:

- Access to, and use of University ICT Services;
- The responsibilities of users regarding the appropriate use of ICT Services; and
- The responsibilities of users in maintaining the good name of the University of Tasmania.

4 Definitions and Acronyms

Access	Connection of University, personal or third party owned Devices to ICT Infrastructure facilities via a direct or indirect connection method. Such connection methods could include but are not restricted to: • LAN/MAN/WAN network connections (e.g. Ethernet); • Wireless network connections; • Remote access via a third party such as a contracted ISP with trusted access to the University network; • Connection via VPN (Virtual Private Networking) technology; and • Connection to any systems, services and applications.

Account	A combination of a username (identifier) and password allocated by an ICT Officer to an Authorised User (the account owner) to access ICT Services, Facilities and Infrastructure.
Algorithm	A cipher used to encrypt and decrypt information using a series of steps that can be followed as a procedure.
Anti-Virus Software	A software package designed to identify and remove known or potential computer viruses, and associated software including but not limited to virus definition files.
Authorised User	An individual who has been granted access to University ICT Services under one or more of the following categories: • A current member of the governing body of the University; • A currently employed officer or employee of the University; • A currently-enrolled student of the University; • Any person granted access to use University of Tasmania ICT Services including, but not limited to: ▪ A contractor undertaking work for the University under the provisions of a legal contract; ▪ A member of a collaborative venture in which the University is a partner; or ▪ A visiting lecturer, student or other associate who is undertaking similar activities in a recognised University, as a registered associate.
Copyright	A form of intellectual property which gives the creator of an original work exclusive rights in relation to that work; and control over its distribution, publication, and adaption.
Data Custodian	A nominated trustee of University of Tasmania data. A data custodian holds responsibility for protecting the data as defined by University of Tasmania Policies and Procedures. Data Custodians may be nominated by their role with the University of Tasmania, or by their role in relation to a ICT Service. A Data Custodian will typically have responsibility for the management of a location of shared information, a database, or an application referencing a database distinct from the role of a systems administrator. Data Custodians may include but are not restricted to: • Application Managers • Data Managers • Business Systems Owners
Device	Any computer or electronic device capable of accessing, storing and communicating data.
Encryption	The process of transforming information using an algorithm to render it unreadable to those without special knowledge (access to a key).
End Host Device	An electronic device which can be connected to a network via the allocation of a network address to that device's MAC address such that this forms the only active network connection on that device. End Host Devices include, but are not limited to: • Desktop computers; • Notebook computers;

	• Workstations; • Servers; • Network Printers; • Telecommunications equipment; • Wireless Devices; and • Other network aware devices.
Facility Manager	Staff member authorised and responsible for managing access to and use of an ICT Facility.
Gateways	Gateways are ICT Services where Device connection has been authorised by the Director, IT Resources. Gateways are provided for the purpose of connecting privately owned Devices, and include: • Uconnect wireless; and • Wired connectivity in some study areas (e.g. Learning Hubs).
ICT	Information and Communication Technologies
ICT Facilities	All computers, terminals, telephones, end host devices, licences, centrally managed data, computing laboratories, video conference rooms, and software owned or leased by the University.
ICT Infrastructure	All electronic communication devices, networks, data storage, hardware, and network connections to external resources such as AARnet and the Internet.
ICT Officer	The University of Tasmania staff authorised by the Faculty, School and/or Director, IT Resources to maintain and/or administer ICT Services, Facilities, Infrastructure, user level accounts and passwords.
ICT Security Framework	The ICT Security Framework refers to all University of Tasmania Policies and Procedures concerning ICT Security.
ICT Security Officer	The ITR appointed representative responsible for ICT security.
ICT Services	All systems supporting interaction, information provision, information storage, or communications provision and the ICT Facilities on which they operate.
Internet	A term for the global computer network used to share information along multiple channels, and over multiple protocols. This definition of Internet is inclusive of protocol driven networks such as the World Wide Web, and all peer-to-peer networks.
ITR	Information Technology Resources
Limited Personal Use	Infrequent, brief and legal use of ICT Facilities for personal, non-commercial purposes during personal time. Personal use activities must not cause offence to other users, or be reasonably considered to cause offence. Personal usage must not disrupt other users or prevent any person undertaking University related work from using ICT Services and Facilities.

Modifications	The disconnection, repair, or connection of devices and the installation or configuration of software or hardware.
Network Modification	Any change to the topology of the University of Tasmania network other than the addition of End Host Devices. Changes include, but are not limited to, the addition, reconfiguration or removal of: • Network Switches; • HUBS; • Routers; • Any network aware device with more than 1 active network connection.
Network Port	Any individual switch port, wall outlet or wireless access port that provides connectivity to the University of Tasmania network.
Port Splitter	Any device attached to a network port that allows simultaneous access through that port. Devices include, but are not limited to: • Switches; • HUBS; • Routers; • Wireless Access Points; • Active Multi-homed computers\devices; • Modems; and • Any network aware device with more than 1 active network connection.
Request for Access to University Services	A process provided by IT Resources to handle requests for access to University ICT Services, Facilities and Infrastructure by non-University personnel.
Senior Officer	• Vice-Chancellor • Deputy Vice-Chancellor (Academic) and Provost • Pro Vice-Chancellor • Executive Director Finance • Executive Director Planning and Development • Director/Principal of University Institute • Dean including the Dean of Graduate Studies by Research • Head of School • Head of Section
Simultaneous Access	Access through one port or wall outlet by more than one End Host Device
University	The University of Tasmania

5 Policy Maker

Director, Information Technology Resources

6 Policy Provisions

ICT Services, Facilities and Infrastructure are provided in support of University business including research, teaching and learning, and operational activities.

The conditions of use defined in this Policy, and associated ICTP Policies and Procedures, apply to all University members, all ICT Services provided by the University, all Facilities and Infrastructure owned by the University, and to any privately owned Device that connects to University Infrastructure.

6.1 Appropriate Use

University of Tasmania ICT Services must be used in an appropriate manner.

Appropriate use is considered to be the use of equipment in:

- a legal manner, meeting the requirements of legislation and University Bylaws, Ordinances and Policy; and
- meeting the principles of fair use.

6.2 Authorised Users

ICT Services and Facilities are only available for use by Authorised Users.

An Authorised User is an individual that has a legitimate relationship with the University of Tasmania as defined in the ICT Access Control Policy.

All Authorised Users are bound by the ICT Services and Facilities Use Policy. The ICT Services and Facilities Use Policy becomes binding when:

- Staff members and associates accept their offer of employment or appointment;
- Students accept an offer of enrolment.

Associate members and other occasional users who are not Staff or Students of the University of Tasmania must sign and return a copy of the UTAS ICT Services and Facilities Use Agreement. The ICT Services and Facilities Use Agreement must be signed and returned to IT Resources in order for any Associate member to be granted Authorised User status.

The UTAS ICT Services and Facilities Use Agreement may be superseded by a usage Agreement, employed by a Division, Faculty, School, Centre, Institute or Section, that has been authorised by a Senior Officer.

Where such an Agreement exists, and it meets the requirements of the UTAS ICT Services and Facilities Use Agreement and extends upon those requirements, that Agreement is binding for the Facilities to which it applies and is considered an extension of the University of Tasmania ICT Security Framework.

6.3 Responsibilities of Authorised Users

University of Tasmania ICT Services must be used in a manner which supports the good name of the University and may only be used:

- in support of teaching, learning, research, personal or professional development, business operations and management or other activities officially directed towards the mission of the University; and
- for limited personal use.

All Authorised Users of University ICT Services must respect the rights of other Authorised Users to ensure that all have equitable privileges, privacy and protection from interference or harassment.

6.4 Access to ICT Facilities

Access to ICT Services and Facilities is provided as per the requirements of the ICT Access Control Policy.

Physical access to ICT Facilities is managed through the University's security arrangements. Access to buildings and computing laboratories is at the discretion of the relevant Facility Administrator.

6.5 Accessing the Internet and Online Services

Access to the Internet, and services provided via the Internet, are available to Authorised Users only.

Use of the Internet and associated services are provided under the conditions of appropriate and ethical use. Users of this service must respect the rights of other Authorised Users to ensure that all have equitable privileges, privacy and protection from interference or harassment.

Internet usage must be legal and comply with the requirements of all Federal and State Government legislation, University Ordinances, Policies, and Procedures.

6.5.1 Internet and Online Services Access Restrictions

The University of Tasmania reserves the right to block access to internet services, or websites, where accessing, or obtaining content from, those services or websites using University of Tasmania ICT Services, Facilities, or Infrastructure would be considered a breach of Federal or State legislation, or a breach of University of Tasmania Policy.

The University of Tasmania reserves the right to block access to any online service which is identified as a platform for the distribution of viruses, malware, other malicious software, or is associated with solicitation of personal or financial information.

The University will make attempts to ensure any internet service, or website, which is blocked is not used for research, teaching and learning, or University business reasons.

All access restrictions will be approved by the Director, IT Resources.

Reviews of access restrictions will be heard by the Director, IT Resources.

6.6 Copyright Provisions

The University of Tasmania expressly forbids the use of any of its ICT Services, Facilities and Infrastructure for any purpose which would breach copyright in any way.

The University considers copyrighted materials to include, but not be limited to:

- Music
- Movies
- Television programs
- Electronic publications
  - Ebooks
  - Electronic journal papers
- Computer software
- Unlicensed data, including unlicensed research data

6.6.1 University of Tasmania ICT Services, Facilities, and Infrastructure Provisions in Relation to Copyright Protected Material

University of Tasmania ICT Services, Facilities, and Infrastructure may not be used to download, copy, compress, store, transfer or redistribute content without the express permission of the copyright owner.

The University reserves the right to remove any alleged infringing material from any of its ICT Services, Facilities, and Infrastructure without prior notification.

Where a service or website, external to the University, is identified as a source of infringing material the University reserves the right to block access to that service or website.

6.6.2 Responsibilities of University of Tasmania Members in Relation to Copyright Protected Material

Members of the University are prohibited from using any University ICT Services, Facilities or Infrastructure to acquire, store or share materials that infringe the rights of the copyright holder.

Members may, on occasion, purchase materials via online distributors using University ICT Services, Facilities and Infrastructure. These materials may be stored on University Facilities in accordance with the licence conditions under which they were purchased.

It is the responsibility of University of Tasmania Members to ensure they manage their copyrighted materials in accordance with legislative and policy requirements.

6.6.3 Dealings in Copyright Protected Material for Teaching or Research

The University holds licences which allow certain copyrighted material, including text, images, music and recorded broadcasts, to be copied, stored and communicated for the educational purposes of the University. Staff and students are obliged to abide by the licence conditions for the use of this material.

The University has made available information regarding the use of copyrighted materials for teaching or research purposes at the following locations on the University's web site:

- http://www.utas.edu.au/policy/subject.html#teaching
- http://www.utas.edu.au/copyright/

Further information regarding the use of copyrighted material for educational purposes may be sought from the University of Tasmania Copyright Officer.

6.6.4 Private Use Conditions and the University of Tasmania

The Copyright Act 1968 provides individuals with some rights regarding Private Use of recordings that they have purchased.

Private Use considerations allow individuals to alter the format of musical recordings that they own so that they may be used on a device that can be used to cause those recordings to be heard.

These considerations are applicable provided that the original copy does not infringe copyright; and that the copy they make is for domestic listening purposes and that the device they copy the music to is their own.

University owned ICT Services, Facilities and Infrastructure are owned by the University; not by individuals. Therefore, regardless of whether an individual owns an original copy of a recording, digital copies may not be stored on any University of Tasmania ICT Service, Facility or Infrastructure item as this act breaches Private Use considerations of the Copyright Act 1968.

Members of the University may use University ICT Facilities and Infrastructure for private listening purposes, but may not store, or distribute materials. Private media libraries must be held on devices owned by the Member.

6.6.5 Notices of Copyright Infringement

The University of Tasmania makes all attempts to ensure copyrighted materials are used within licence conditions, and that ICT Services and Facilities are not used to facilitate copyright breach.

All materials, including non-infringing materials, and ICT equipment are subject to removal from the University of Tasmania network in the event that a notice of copyright infringement is delivered against the University.

Should the University receive a notice of copyright infringement the University reserves the right to remove the material in question, or make it unavailable by disconnecting the underlying ICT Infrastructure via logical or physical action, until such time that a determination about the legitimacy of the infringement claim can be made.

Notices of copyright infringement, or takedown notices, may be lodged by contacting relevant ICT Officers or via the following location on the University's web site:

- http://www.utas.edu.au/copyright/feedback/takedown.html

6.7 Modification of ICT Services, Facilities and Infrastructure

Network modifications shall only be made following written approval by the Director, IT Resources or their nominees.

Network modifications may only be carried out by an ICT Officer.

6.7.1 Unauthorised Modifications of ICT Services, Facilities and Infrastructure

All network modifications performed without authorisation from a Senior Officer or by an unauthorised person are prohibited.

Unless part of an approved network modification under section 6.7 above, the installation of a port splitter or any network communication device that supports multiple simultaneous connections to a single network port or third party networks is expressly prohibited.

Examples of modifications include, but are not limited to:

- Disconnecting computers from the University network;
- Connecting unregistered devices;
- Connecting hubs, switches or port splitters.

Where an unauthorised modification is detected, a breach of policy may be pursued and connectivity to a network port may be terminated.

6.8 Use of Privately Owned ICT Devices

The University of Tasmania allows Authorised Users to connect privately owned Devices to the University of Tasmania ICT Infrastructure via connection Gateways, and allows limited connection to the University of Tasmania staff network.

6.8.1 Connection to Gateways

Gateways are ICT Services where Device connection has been authorised by the Director, IT Resources. Gateways are provided for the purpose of connecting privately owned Devices, and include:

- Uconnect wireless; and
- Wired connectivity in some study areas (e.g. Learning Hubs).

Any Device that connects to a University of Tasmania Gateway must meet the following requirements:

- Privately owned Devices may only be used on the University of Tasmania Gateways in a legal manner and in accordance with Federal and State legislation.
- Users must adhere to University of Tasmania Ordinances, Policies and Procedures whist connected to any University of Tasmania Gateway.
- All Devices that support anti-virus software must have an up-to-date anti-virus package installed and operating while connected to the University network.

The University of Tasmania shall not be held responsible for the management and maintenance of privately owned Devices connected to Gateways.

6.8.2 Connection to the University of Tasmania Staff Network

University of Tasmania Gateways are distinct and separate networks from the University of Tasmania staff network.

In cases where a privately owned Device is to be registered on the University of Tasmania staff network the following conditions apply:

- The connection request must be supported by a valid reason, and made to a Senior Officer.
- Connections must be authorised by the Senior Officer.
- Access will be provided on a minimal requirements basis.
- Devices must have an up-to-date anti-virus package installed and operating.
- Devices must be used in a legal manner and in accordance with Federal and State legislation.
- Users must adhere to University of Tasmania Ordinances, Policies and Procedures whist connected to the University of Tasmania staff network.

An ICT Officer must be able to provide connection support to the Device while it is connected to the University of Tasmania staff network:

- The owner of the Device must provide an account to the ICT Officer.
- In cases where the support of a privately owned Device extends beyond connection, the Device owner may be charged remuneration for that support. The charge for support is at the discretion of the Faculty, School or Division providing the connection.

6.8.3 Connection Restrictions

No privately owned Device will have access to student databases, staff databases or financial systems, except where those systems provide a self service interface for the User.

Privately owned Devices may only have access to ICT Services or data stores where the Data Custodian authorises such a connection to occur, or the ICT Service or data store provides a self service interface for the User.

6.8.4 Connection Disclaimers

The University of Tasmania shall not be held responsible for damage or loss to privately owned Devices.

The Director, IT Resources, has the right to negotiate with any Senior Officer regarding the authorisation of a connection request for a privately owned Device to the University of Tasmania staff network. Through negotiation the Director, IT Resources, has the right to reject or revoke any connection request.

ICT Officers have the right to disconnect privately owned Devices from University of Tasmania Gateways and network in the event of a breach of this Policy or any other Ordinance, Policy or Procedure of the University of Tasmania.

The ICT Security Officer has the right to request disconnection of any privately owned Device connected to any Gateway or network of the University of Tasmania.

6.9 Software Installation on University of Tasmania ICT Facilities and Devices

University of Tasmania ICT Facilities and Devices operate with a standard, or known, operating environment. This environment is created and configured to allow a Device

to support Authorised Users in their work, and to integrate with University of Tasmania ICT Services.

Any changes to this environment, such as additional software or configuration changes, must be authorised, and preferably actioned, by an ICT Officer.

6.9.1 Authorised Software

Authorised software is considered to be software that meets the following conditions:

- The software is used in accordance with licence terms;
- The software has been tested by an authorised ICT Officer to ensure functionality and security of ICT Facilities;
- The software has been installed by an authorised ICT Officer; or
- The installation of the software has been authorised by an ICT Officer.

6.9.2 Unauthorised Software

Unauthorised software is considered to be any software that:

- Is used in breach of software licence agreements;
- Has not been tested by an authorised ICT Officer;
- Is not installed by an ICT Officer; or
- Has not been authorised by an ICT Officer.

6.9.3 Unlicensed Software

Unlicensed software is considered to be all software used outside of the licence agreement that accompanies the software.

The use of unlicensed software on University of Tasmania ICT Facilities is strictly prohibited, and any instance immediately renders the software unauthorised.

The installation and use of unlicensed software can not be authorised by any person. The software may not be installed or used until the conditions of the licence have been met.

Any software installed or used in violation of licence terms shall be deemed unauthorised software and will be in breach of this policy.

6.10 Monitoring of ICT Services, Facilities and Infrastructure

All usage of ICT Services, Facilities and Infrastructure will be monitored.

Information related to the usage of ICT Services, Facilities and Infrastructure will be stored and may be used to ensure or investigate compliance with University Policies, Procedures and Guidelines and relevant State and Federal legislation, the University of Tasmania may collect information related to the use of ICT Services, Facilities and Infrastructure.

Further information related to the monitoring of ICT Services, Facilities and Infrastructure, and the usage of information collected, is provided in the ICT Security Policy.

6.11 Privacy

Information related to the use of University of Tasmania ICT Services and Facilities is collected and may be consulted to ensure compliance with University policies, procedures and guidelines, and relevant State and Federal legislation. This information may be accessed for purposes of investigating allegations of misuse.

Information may be provided to law enforcement agencies where necessary to investigate or report suspected unlawful activity, as per the University of Tasmania Privacy Policy.

6.12 Breaches

Breach of this Policy may result in disciplinary action, as provided for under the applicable Employment Agreements and Ordinances.

Staff, students and associates learning of any violation of this Policy are obligated to bring this matter to the attention of an appropriate staff member within the University without delay.

7 Supporting/Related Documents

- Ordinance 9 Student Discipline
- Current Academic and General Staff Agreement(s)
- Information Technology Infrastructure Library (ITIL)
- ISO 27000 (ISO 27002)
- Privacy Policy
- Records Management Policy
- Risk Management Policy

8 Key Words

- Acceptable Use
- Usage Agreement
- Security
- ICT
- Information
- Technology

9 Supporting Procedures/Guidelines

- ICT Services and Facilities Use Agreement
- Blacklisting Procedure

RESPONSIBILITIES

Implementation	Director, ITR
Compliance	Director, ITR
Monitoring and Evaluation	ICT Security Officer ICT Staff, External Audit
Development and/or Review	Director, ITR ICT Security Officer

Interpretation and Advice	ICT Security Officer Governance and Legal

WHO NEEDS TO KNOW THIS POLICY?

All staff, students and associates.

EFFECTIVENESS OF THIS POLICY

The effectiveness of this policy shall be established through regular audit.

POLICY HISTORY

Policy No.	ICTP 3.1
Approved / Rescinded	Approved by Council
Date	June, 2010
Council Resolution Number	10/3/43