VICTORIA UNIVERSITY
MELBOURNE AUSTRALIA

# POLICY AND PROCEDURES

## Appropriate Use of ICT

This policy is important to:

- All Staff members
- All Students using Information Technology Facilities

| | |
|---|---|
| POLICY NUMBER: | POI120427000 |
| DATE APPROVED: | 4 April 2012 |
| POLICY CATEGORY: | General (Information and Communication Technology) |
| POLICY OWNER: | Pro Vice-Chancellor & Chief Information Officer |

## 1. CONTEXT

Information Technology Facilities are described as an amalgam of voice, data and computing facilities built over a physical cabling and wireless infrastructure to provide electronic communications and data processing capability in order to support the University's day to day operations.
This policy applies to all Information Systems and Services, including but not limited to, computer equipment, software, operating systems, storage media, communication facilities (Voice, Video and Data), network accounts, email accounts, Web browsing (from the University network) are the property of the University. These systems are to be used for business purposes in serving the interests of the University, and of our clients and students in the course of normal operations.

Information Technology Services has been charged with the responsibility to install and maintain IT and communications equipment and physical infrastructure vital to carry out the core business of the University. A set of policies and guidelines has been enacted to protect vital assets and minimise the risk of disruption to teaching, research and University business in general.

It is the responsibility of every staff member and persons under their direction (students, contractors, visitors and the like), as Authorised Officers of the University, to make themselves aware of these guidelines and related information technology policies published on the University Web, and to conduct their activities accordingly.

An Appropriate Use Policy is not intended to impose restrictions contrary to the basic philosophy of the University, and a university culture of debate, openness, trust and integrity, but rather as a formal statement defining obligations, restrictions and responsibilities necessary to protect the University's staff, students, affiliates, agents, the wider community and the institution itself from illegal or damaging actions by individuals, either willfully or through ignorance.

## 2. DEFINITIONS

2.1 Authorised Officer: Any person directly or indirectly employed by the University and authorised to act on the University's behalf.

2.2 Communications equipment: Electronic devices such as network switches, routers, Telephony and the like, offering the means for voice and data communications between people.

2.3 ICT: Information, Communication & Technologies

2.4 ITS: Information Technology Services

2.5 Physical infrastructure: Communications cabling such as copper and fiber optic cables and associated infrastructure such as communications racks, cabling pathways and conduits.

2.6 Reasonable personal use: Personal use of IT facilities and services which is minor or incidental.

2.7 Spam: Unauthorised and / or unsolicited electronic mass mailings

2.8 Spoofing: An individual masquerading as someone else, especially when sending electronic communications

2.9 University: Victoria University

2.10 Uptime: A measure of system availability expressed as % of the total time period

## 3. STATEMENT OF POLICY

### 3.1 Usage

3.1.1 Under no circumstances is any user authorised to engage in any activity that is illegal under state, federal or international law while utilising The University owned or managed resources. Staff are expected at all times to comply with the Staff Code of Conduct

3.1.2 Under no circumstances should any person using the University's Information Technology facilities, violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations. This includes, but is not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the University.

3.1.3 While the University respects a reasonable level of confidentiality, users should be aware that the data they create on corporate systems, including the communications infrastructure and desktop computers, remains the property of the University. Because of the need to protect the University's network, servers, and data (including intellectual property), management may be required, from time to time, to intercept, interrogate, or otherwise capture data created or received by individual users.

These actions will be performed by a limited set of authorised individuals within Information Technology Services. Specific cases where this may be necessary are given in companion policies. See ITS Staff Audit Authorities Policy

3.1.4 The use of the University's Information Technology facilities for unauthorised commercial or private gain is strictly prohibited.

3.1.5 Users are responsible for exercising good judgment regarding their reasonable personal use, with guidance from: -

- Teaching staff and Student Services for students, and
- Individual departmental managers and in particular Heads of Department for others.

This especially applies to use of the external Web where costs are directly incurred by the institution. Resources are made available for legitimate University business and operations where a small amount of private use is tolerated. Legitimate University business includes teaching, research and independent study. Costs incurred by the University through excessive personal use may be recovered directly from the individual concerned, and may lead to further disciplinary/legal actions.

3.1.6 Users are expected to comply with any local rules governing shared information technology resource spaces, such as PC Laboratories or laptop docking areas. In particular: eating, drinking, or smoking in a computer laboratory is prohibited; users must not behave in a noisy, offensive or other disruptive manner; users must keep shared work environments tidy (e.g. disposing waste paper in recycle bins); respect the rights of others (e.g. preventing others from reasonable access to resources by non-work related use of PCs, excessive printing, stealing consumables such as paper).

3.1.7 Desktop and laptop computers must not be the sole repository of corporate, teaching or research data. All such data must be stored on faculty/divisional network drives, and new work backed up to the network as soon as possible. (See Backup Recovery Policy)

3.1.8 Configuration changes to IT Facilities and physical infrastructure are the responsibility of ITS and their Authorised Officers. Unauthorised tampering with any part of IT infrastructure is strictly prohibited.

3.1.9 Telephones must not be used for any unlawful purpose. Staff are required to follow the Staff Code of Conduct when using their IP Phones.

## 3.2 Security and Proprietary Information

3.2.1 Users should keep passwords secure and it is not permissible to share accounts except where exempted by other policies. Revealing your account password to others or allowing use of your account by others is prohibited. This includes family and other household members when work is being done at home. Authorised users are responsible for the security of their passwords and accounts, and further are responsible for any infringement carried out by any third party given access to their accounts.

3.2.2 Users should never provide confidential or personal information over the Internet in response to unsolicited inquiries. Legitimate organisations like banks will never send such an unsolicited email request. Users should be wary of clicking on Web sites embedded in emails as this may redirect them to a malicious site. If ITS identifies an account as being compromised it will be locked out immediately and the account owner informed.

3.2.3 Staff should consider the sensitivity of any information or data transmitted across the internal and external network, and classify it as confidential or non-confidential. Deciding whether data or information is confidential rests with the user taking into account other governing regulations and policies of the University, see Central Policy Register. Examples of confidential information include but are not limited to: student and staff personal data, examination results, information covered by

University's Privacy and Intellectual Property regulations, confidential senior management communications, specifications of commercialised University developments or patents, vendor lists, details of commercial contracts and agreements, and research data restricted by privacy and ethical concerns. Staff should take all necessary steps to prevent unauthorised access to such information and use relevant secure modes of communication. See Privacy Policy

3.2.4 Sensitive information held on desktops or transmitted across the Internet should be encrypted and sent over a secure network connection. Because information contained on Laptop computers is especially vulnerable, additional special care should be exercised.

3.2.5 All staff and student hosts (including desktops and laptops) connected to the University network, whether owned by the staff member or the University have the current operating system patches applied to them, and continually executing approved virus-scanning software with a current virus database. Users who continually inject viruses into the University's infrastructure may be denied access.

## 3.3 Prohibited Activities

The following activities are prohibited (unless specific written permission is obtained from the Director of Information Technology Services):-

3.3.1 Victoria University computers and networks must not run software unless it comes from trusted sources subject to section 5.22 of the High Level Information Security Policy.

3.3.2 The use of unlicensed software, and the playing of computer games using illegal or copied media and software on workstations or laboratory computers is strictly prohibited. See, Licensing and Use of Computer Software policies

3.3.3 Deliberate introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

3.3.4 Making fraudulent or unapproved offers of products, items, or services originating from any The University asset or service (e.g. offering access to University services for personal benefit).

3.3.5 Making statements about warranty, guarantees, or similar binding commitments on behalf of the University, expressly or implied, unless it is a part of normal job duties.

3.3.6 Deliberately effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the client is not an intended recipient or logging into a server or account that the user is not expressly authorised to access, unless these activities are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

3.3.7 Port scanning or security scanning is expressly prohibited unless prior approval has been granted by Information Technology Services. This also applies to the execution of any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the normal job/duty, or otherwise approved by Information Technology Services.

3.3.8 Circumventing user authentication or security of any host, network or account.

3.3.9 Interfering with or denying service to any user other than the individual's host (for example, denial of service attack).

3.3.10 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, any user's terminal session, via any means, locally or via the external Web. This applies to sessions anywhere on the Web (i.e. it includes hacking sessions on external Web addresses).

3.3.11 Providing information about, or lists of, The University staff and students to parties outside the institution, unless it is expressly part of normal duties.

3.3.12 Deliberate modifications to the current production network.

### 3.4 Physical Security

Physical information technology resources of the University must be kept secure and not damaged in any way. This covers:

3.4.1 Unauthorised access to any University information technology assets (e.g. Communications room, Computer operation rooms (Data Centre's), computer and communications systems, etc.) within the University, or elsewhere, without proper authorisation from ITS is strictly prohibited.

3.4.2 Unauthorised access to any University restricted area where information technology assets are stored or installed without proper authorisation from ITS is strictly prohibited. Security Access to Controlled Areas in IT Policy

3.4.3 Willfully or through negligence, damage or alter the arrangement of any hardware, software, physical plant, or communications component without proper authorisation from ITS is strictly prohibited.

3.4.4 Unauthorised tampering with terminals, personal computers or any other associated equipment without proper authorisation from ITS is strictly prohibited.

3.4.5 Communications room must be kept secure and must be maintained to be in the proper conditions that allow it to operate well and conform to relevant standards and guidelines at all times. Installation of new racks, wire, hardware or other peripherals and modification to existing arrangements within Communications room must be done carefully, and done by people with enough knowledge, care and understanding, thus must be authorised, advised and closely monitored by ITS. Unauthorised access by any person including unauthorised Victoria University staff is strictly prohibited. Violation can result in a big risk and jeopardize the university operation and as such will be subject to serious disciplinary action at the highest possible level.

### 3.5 Telecommunications Security and Safety

3.5.1 The design must conform to the following applicable standards.

- AS/NZS 3000:2007 (supersede AS/NZS 3000:2000) - The Australian/New Zealand Standard for Wiring Rules.
- AS/NZS 3084:2003 - Telecommunications installations - The Australian/New Zealand Standard for Telecommunications pathways and spaces for commercial buildings.
- DR 07135 CP - Amendment 1 to AS/NZS 3084:2003 - The Australian/New Zealand Standard for Telecommunications installations - Telecommunications pathway and spaces for commercial buildings (ISO/IEC 18010:2002, MOD)
- AS/ACIF S008:2006 (supersede AS/ACIF S008:2001) - The Australian Communications Industry Forum Standard for Requirements for customer cabling products.
- AS/ACIF S009:2006 (supersede AS/ACIF S009:2001) - The Australian Communications Industry Forum Standard for Installation requirements for customer cabling (Wiring Rules)

3.5.2 The design must also conform to ITS's Guidelines For The Design Of Telecommunications Spaces And Pathways In Victoria University Buildings. If any conflict exists among the standards mentioned above or between the standards mentioned and this document, then the conflict must be brought to the attention of the Victoria University Telecommunications Project Manager for resolution.

3.5.3 Design of new buildings or extensive renovation to buildings must be submitted to ITS for reviews, comments and approval before proceed to construction phase.

### 3.6 Requests for the new installation of communications and network connectivity

ITS is responsible for providing new installations and communications systems connectivity. However, in many cases, it is subject to the availability of required connecting ports (voice and/or data). Installation of new ports depends on many factors including, but not limited, to the availability of related communications devices to provide extra ports (voice and/or data), and the available capacity to install required and relevant new devices into Communications rooms. To avoid undue delay, and possibly long delay as well as substantial extra cost, request for ITS services must allow sufficient time for proper preparation and arrangement

## 4. PROCEDURES

Any procedure associated with aspects of this policy may be found at the ITS Policy website or by enquiry to the ITS Service Desk.

## 5. POLICY ADVISOR

Associate Director Enterprise Services, Information Technology Services

## 6. RELATED POLICIES AND LEGISLATION

### 6.1 Related Standards

AS/NZS 3000:2007 (supersedes AS/NZS 3000:2000) - The Australian/New Zealand Standard for Wiring Rules

AS/NZS 3084:2003 - Telecommunications installations - The Australian/New Zealand Standard for Telecommunications pathways and spaces for commercial buildings

DR 07135 CP - Amendment 1 to AS/NZS 3084:2003 - The Australian/New Zealand Standard for Telecommunications installations - Telecommunications pathway and spaces for commercial buildings (ISO/IEC 18010:2002, MOD)

AS/ACIF S008:2006 (supersedes AS/ACIF S008:2001) - The Australian Communications Industry Forum Standard for Requirements for customer cabling products

AS/ACIF S009:2006 (supersedes AS/ACIF S009:2001) - The Australian Communications Industry Forum Standard for Installation requirements for customer cabling (Wiring Rules

Guidelines For The Design Of Telecommunications Spaces And Pathways In Victoria University Buildings

### 6.2 Related Policies

Security Access to Controlled Areas in IT (POI100929000)
ITS Staff Audit Authorities Policy (POI110330003)
Use of Email (Staff and Students) (POI111004003)
High Level Information Security Policy (POI110817000)
Computer Software: Licensing and Use of (POI120314003)
Connecting Devices to VU Data Network (ITi-P2006-46)
Privacy Policy (POU110803000)
Staff Code of Conduct (POH111221000)

All University policies are recorded in the Central Policy Register,
A list of all existing IT Policy related documents (i.e. ITu, ITi, ITg and ITo) are published on the ITS Policies Web Page

### 6.3 Relevant Legislation

The Privacy Act 1988;
The Crimes Act 1914;
The Copyright Act 1968; and
The Freedom of Information Act 1984.

### 6.4 Acknowledgement

SANS (SysAdmin, Audit, Network, Security) Institute http://www.sans.org/resources/policies

## 7. CONSULTATION AND ACCOUNTABILITIES

### 7.1 Consultation

7.1.1 ITS Department, IT Advisory Committees
7.1.2 Information Knowledge Management Committee (IKMC)
7.1.3 University-wide consultation
7.1.4 Approval by Vice-Chancellor

### 7.2 Accountabilities

7.2.1 RESPONSIBILITY
Pro Vice-Chancellor and Chief Executive Officer, for the operational management of the policy

7.2.2 IMPLEMENTATION PLAN
Each Branch of Information Technology Services (Enterprise Services, Enterprise Solutions, IS Service Quality) will be responsible for the implementation of this policy.

7.2.3 TRAINING PLAN
To avoid vicarious liability accusations the University must clearly disseminate this policy to all students, staff and agents of the University. As a minimum this policy statement will be:
Made available and notified to all new staff as part of their induction program. This must include casuals and work placements.
Made available and notified to all students on their first enrolment to the University.
Made available and notified to all agents or visitors of the University who are given access to the University's email and voicemail infrastructure.
Published through the internal University Web (Intranet).
Referenced in the University's Human Resources Manual.
Be published through the University's Policy Database.

7.2.4 COMPLIANCE

Staff users of University information technology resources found to have violated this policy will be subject to disciplinary action, up to and including termination of employment or legal action.

Students found to have violated this policy will be subject to disciplinary action, up to and including termination of their enrolment or legal action.

Other users, such as consultants, who have violated this policy, will be subject to appropriate action up to and including legal charges.

7.2.4 EFFECTIVENESS OF THIS POLICY

There will be periodic checks to ensure that this policy is being adhered to.

## POLICY HISTORY

| Version approval date | Summary of changes |
|---|---|
| 4 April 2012<br>*(POI120427000)* | Reviewed policy. |
| 27 May 2011<br>*(POI110603001)* | Amended via minor amendments – including renaming to Appropriate Use of ICT. |
| 4 July 2008<br>*(POI110603000)* | Amended via Review |
| 1 June 2006<br>*(POI08063000)* | Minor Amendments – reformatting and update of definition of ‘software’. |
| 9 May 2005<br>*(POI050524002)* | Major amendments – including renaming to Appropriate Use of Information Technology Facilities |
| 7 May 2003<br>*(POI040809002)* | New Policy – Policy on Use of University’s Computing Facilities |