SECTION 15

POLICIES - APPROPRIATE USE OF IT FACILITIES & EMAIL

15. POLICIES - APPROPRIATE USE OF ICT & USE OF EMAIL (STAFF AND STUDENTS)

STUDENTS ARE REQUIRED TO COMPLY WITH ALL VICTORIA UNIVERSITY POLICIES AND PROCEDURES. BELOW ARE RELEVANT PARTS OF TWO ITS POLICIES. ALL ITS POLICIES CAN BE FOUND AT THE ITS POLICIES SITE http://intranet.vu.edu.au/its/Policies/

15.1 POI110603001 APPROPRIATE USE OF ICT

This policy outlines to the University community what is considered appropriate use of the University's IT facilities. The important parts of the policy are listed here. To see the full policy please go to the Central Policy Register: http://wcf.vu.edu.au/GovernancePolicy/PDF/POI080630000.PDF

15. POLICY

15.1 Usage

15.1.1 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

15.1.2 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.

15.1.3 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

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

15.1.5 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.

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).

15.1.6 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)

15.1.7 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.

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

15.2 Security and Proprietary Information

15.2.1 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.

15.2.2 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.

15.2.3 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

15.2.4 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's are especially vulnerable, additional special care should be exercised.

15.2.5 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.

15.3 Prohibited activities

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

15.3.1 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.

15.3.2 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

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

15.3.4 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).

15.3.5 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.

15.3.6 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.

15.3.7 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.

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

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

15.3.10 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).

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

15.3.12 Deliberate modifications to the current production network.

15.4 Physical Security

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

15.4.1 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.

15.4.2 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

15.4.3 Wilfully 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.

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

15.4.5 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

15.5 Telecommunications Security and Safety

15.5.1 The design must conform to the following applicable standards:-

- AS/NZS 3000:2007 (superseded 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)

15.5.2 The design must also conform to ITS's Design of Telecommunication Spaces and Pathways. 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.

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

15.6 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

Since the cost resulting from not taking Telecommunications Security seriously is high, failure to conform to this part of this policy will be subject to the University's highest level disciplinary actions.

15.2 POI111004003 USE OF EMAIL (STAFF AND STUDENTS)

The purpose of this policy is to ensure the proper use of the University's email system and make users aware of what the University deems as acceptable and unacceptable use of its email system. The important parts of the policy are listed here. To see the full policy please go to the Central Policy Register: http://wcf.vu.edu.au/GovernancePolicy/PDF/POI040809005.PDF

15 POLICY

15.1 Legal Requirements

Under no circumstances is any e-mail user authorised to engage in any activity that is illegal under state, federal or international law while utilising the University's owned or managed resources, or provided to them via an external host or manager of that system.

Furthermore, email users must ensure all legislation and policies relating to Equity and Diversity are strictly followed. Relevant Legislation includes, but is not limited to:

- Racial and Religious Tolerance Act (Vic) 2001
- Equal Opportunity Act (Vic) 2010
- Age Discrimination Act (Cth) 2008
- Sex Discrimination Act (Cth) 1984
- Race Discrimination Act (Cth) 1975
- Disability Discrimination Act (Cth) 1992

Related Policies and documents staff and students must adhere to include;

- Discrimination/Harassment and Bullying Policies and Procedures for Staff
- Staff Code of Conduct
- Equity and Diversity Plans and Strategies for staff
- Student Charter

The following actions are forbidden by law when sending or forwarding emails

- Using material which constitutes an infringement of copyright. Refer to the University's 'Copyright Material (Use of)' policy in determining what third party material can be used
- Defaming an individual, organisation, association, company or business
- Communications that are obscene, offensive or involve the use of illegal material, including the use or transfer of material of a sexual nature
- Breaching a university policy, procedure, statute or regulation
- Directly or indirectly interfering with or conflicting with lawful University business
- Intentionally bringing the University or its officers into disrepute
- Sending unsolicited and unauthorised global or commercial email messages
- Forging or attempting to forge email messages
- Sending email messages using another person's email account

Any emails received of this nature should be forwarded via email for reporting and investigatory purposes to the ITS Security Office at itsso@vu.edu.au. All email forwarded to the ITS Security Office must be marked as high importance. Each case will be assessed and proper action will be taken based on the severity of the breach.

Staff and students at VU undertaking research may send emails containing such materials provided that it demonstrably refers to their area of research and is done so in a responsible manner.

15.2 Personal Use

Although the University's email system is meant for business use, the University allows the reasonable use of email for personal use:

- Personal use of email should not interfere with work
- Personal emails must adhere to this policy
- The forwarding of chain letters, junk mail, jokes and executables is strictly forbidden
- Must not be used to run a private business whether for profit or non-profit

15.7 Spam

The sending of unauthorised and unsolicited global or commercial email transmissions (spam) is forbidden.

15.8 Sensitive and restricted information

Avoid sending sensitive and restricted official information by e-mail. If you do, you should secure the information by including it in a Microsoft Word or Excel file and protecting it with a password, and then provide the recipient with the password by means of other communication, for instance by telephone. The University recommends any information users consider sensitive or vulnerable be encrypted, especially for transmission to external organisations.

15.9 Disclaimer

The following disclaimer will be added to each outgoing email: 'This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of Victoria University. Finally, the recipient should check this email and any attachments for the presence of viruses. Victoria University accepts no liability for any damage caused by any virus transmitted by this email.'

15.10 System Monitoring

Your emails may be monitored for the operational integrity of the Victoria University Infrastructure and/or to comply with legal or regulatory requirements. The policy for this is set out in the IT Audit Authorities Policy. If there is evidence that a student or staff member is not adhering to the guidelines set out in this policy, the University reserves the right to take disciplinary action, including termination and/or legal action.

15.11 Passwords

All Email accounts maintained on the University's email systems are property of the University. Passwords must not be disclosed to other people unless it is necessary for approved operations of the University. In certain cases it may be necessary, in the interests of the staff member or the University, to reset a password. 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. The University will NEVER ask you to provide your email username and password by email. If you receive a message asking you to respond with details of your username and password, it is a forgery. If you provide these details to third parties fraudulently masquerading as University officials, you will be responsible for all actions carried out using your account by those third parties.