



Name: **Information Technology Systems Acceptable Use**

Approved by: Executive Committee

Last reviewed: 21 May 2009

SECTION 1 - INTRODUCTION _____ 2

 PURPOSE _____ 2

 SCOPE _____ 2

 DEFINITIONS _____ 2

 LEGISLATIVE CONTEXT _____ 3

SECTION 2 - POLICY _____ 4

 PRINCIPLES _____ 4

SECTION 3 - PROCEDURE _____ 10

 PROCEDURE _____ 10

 SUPPORTING DOCUMENTATION _____ 10

SECTION 4 - GOVERNANCE _____ 11

 RESPONSIBILITY _____ 11

 VERSION CONTROL AND CHANGE HISTORY _____ 11

 POLICY & PROCEDURE DIRECTORY REQUIREMENTS _____ 11

SECTION 1 - INTRODUCTION

PURPOSE

This policy sets out the terms and conditions for the use of Swinburne University of Technology (thereafter referred to as "the University") information technology network for the purpose of electronic communication by staff, students and associated bodies in support of the academic, teaching and research enterprise of the University, including news, mail, and ancillary materials relevant to the aims and objectives of the University.

Breaches of this policy will be regarded as a serious matter and the University may take disciplinary or legal action where conditions of use have been found to be breached.

Any reference in this policy to an Act, law, Code of Conduct or other document includes a reference to the Act, law or document as amended from time to time.

SCOPE

This policy applies to all users of the University network or University equipment, which includes but is not limited to all staff, students, part-time staff, and casuals of the University. Use of the University information technology network includes all transmissions to or through the University network.

The Information Technology Services Acceptable Use Policy covers all computers, computing laboratories, lecture theatres and video conferencing rooms across the University together with use of all associated networks, internet access, email, hardware, dial-in access, data storage, computer accounts, software, telephony services and voicemail (the IT facilities').

The University retains the right to access and monitor electronic communications created sent or received by staff or students using the University electronic communications network.

DEFINITIONS

Word/Term	Definition
Authorised person	A person authorised by the Pro Vice-Chancellor.
Electronic communications	Electronic communications includes but is not limited to: <ul style="list-style-type: none">i. Publishing and browsing on the Internetii. Electronic mail ('email')iii. Electronic bulletin/notice boardsiv. Electronic discussion/news groupsv. File transfervi. File Storagevii. Video conferencingviii. Streaming mediaix. Instant messagingx. 'Chat' facilitiesxi. Provision of information via online systemsxii. Online subject delivery systemsxiii. VOIP telephonesxiv. Network devices

Head of Management Unit	Head of Office, Division, School or Department in Swinburne University of Technology (Sarawak Campus)
Users	Includes but is not limited to all staff, students, contractors, casuals and volunteers of the University.
Personal Information	Information or opinion about a person whose identity is apparent or can reasonably be ascertained from the information or opinion.
Sensitive Information	Includes information or opinion about a person's health, racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of professional or trade associations, membership of a trade union, sexual preferences or practices, or criminal record.
Network	A group of computers and peripheral devices (eg printers, modems, VOIP telephones, all other network devices) connected to allow users to communicate and share information and resources including any combination of voice, video and/or data between users.
User Account	A user account is an authorised area within a computer system, which allows a user to access certain system resources such as disk, printing and network services (e-mail, NEWS etc). Access to this account requires a user-ID and password.
NEWS	The Internet NEWS system is an interactive service, which allows users to receive and post information relating to most areas of human endeavour. Topics covered range from humanities to computer science and include both recreational and educational information.
User-ID	The user-ID is a unique alphanumeric string allocated by the system administrator and used to identify a computer system user. The user-ID is used in conjunction with a secure password to gain access to a computer system.
Password	An alphanumeric string assigned by an individual user for the purpose of gaining access to a computer system. Used in conjunction with the user-ID the password must be unique and protected at all times by the user.
Staff	Any person employed by the University

LEGISLATIVE CONTEXT

Name	Location
Communications and Multimedia Act 1998	
Trade Marks Act 2000 (Amended)	

SECTION 2 - POLICY

PRINCIPLES

This policy outlines the principles governing proper and efficient use of electronic communications in order that the University is protected from problems such as error, fraud, defamation, breach of copyright, unlawful discrimination, illegal activity, privacy violations and service interruptions.

1.	Policy Awareness
	<p>1.1 It is the responsibility of the Manager, Student Operations, Manager, Human Resources and Manager, Information Technology Services to ensure that the persons to whom this Policy applies are aware of this Policy. This should include, but is not limited to -</p> <ul style="list-style-type: none">(a) Providing a copy of the policy in staff induction materials,(b) Clear reference to the policy in appropriate student enrolment literature,(c) Regular and timely reminders of the need for compliance with the Policy,(d) Providing updates or developments of the Policy,(e) Establishing a link to the policy upon access to the University system,
	<p>1.2 It is the responsibility of individuals to abide by the Policy.</p>
2.	Authorised Access and Use
	<p>The University permits the use of the University information technology network through local access by staff, and students who have valid accounts created which uniquely identify the user of the account.</p> <p>The University's information technology network is primarily a University tool to be used for University purposes by students and staff. This will include communication relevant to:</p> <ul style="list-style-type: none">• Employees - their employment with the University; or• Students - their enrolment or course activities;• Other parties (including contractors or nominated position holders) - the purpose for which they have been given access to resources
	<p>2.1 Except as provided for in 2.2 the network must:</p> <ul style="list-style-type: none">• only be used for University purposes, or where authorised or required by law, or with the express permission of an Authorised Person, and• be used like other University communications and comply with any codes of conduct which apply to the user, such as the University Code of Conduct.
	<p>2.2 Users of the University network may use electronic communications for limited personal use as long as this does not interfere with their role within the University. Unreasonable or excessive personal usage constitutes a failure to abide by this policy and may result in the consequences set out in paragraph 3.</p>
	<p>2.3 Subject to limited personal use in accordance with clause 2.2, electronic communications must not be used to conduct private business or private commercial transactions, gamble, or carry out excessive and regular research into non-work related topics.</p>
	<p>2.4 Subscribing to list servers (LISTSERVS), mailing lists and other like services must be for University purposes or related professional development reasons only.</p>

	2.5 On-line conferences, discussion groups or other like services must be relevant and used for University purposes or related professional development activities. Such interaction requires that Internet etiquette should be observed along with current societal standards for respect and fairness.
	2.6 Large downloads or transmissions should be minimised to ensure the performance of electronic communications by other users is not adversely affected.
	2.7 The rules governing academic freedom will apply to the use of the University information technology system, where the objective is the transmission and pursuit of knowledge.
	2.8 University Official Communications. E-mail is an official method of communication to University staff. Mass electronic communications, official or otherwise, should only be sent in accordance with normal University procedures. Staff should not disable the receiving of official mail.
	2.9 Staffs are advised to exercise caution in the use of electronic communications to send confidential memos or other commercial-in-confidence information.
3.	Non-Compliance (Breaches)
	<p>Non-compliance with this Policy will be regarded as a serious matter and the University may take disciplinary action including revoking or restricting any right to use electronic communications, cautioning, or, in appropriate circumstances, may lead to more serious disciplinary action in accordance with University disciplinary policies and/or legal proceedings.</p> <p>A failure to comply with this Policy by a staff member will be referred to the Manager, Human Resources or Head of Management Unit in the case of non-employees eg. a contractor or casual staff member and dealt with in accordance with processes in relation to misconduct or unsatisfactory performance (whichever applicable).</p> <p>Examples of non-compliance are included below at 4. Unauthorised Access and Use</p> <p>A failure to comply with the Policy by a student will be dealt with in accordance with the University policy: General Misconduct.</p>
4.	Unauthorised Access and Use
	Unauthorised access and use includes those actions which are not within the boundaries of normal and appropriate practice which includes, but is not limited to:
	4.1 Any unauthorised interception, reading, copying or modifying of electronic data on University information technology systems will be in breach of this policy and subject to disciplinary and/ or legal proceedings. This will include unauthorised access, creation, modification or deletions of student records, human resource systems, payroll, financial records, library systems and any other access to University electronic systems.
	4.2 Any attempt to circumvent the user authentication or security of any host, network or account. This includes the distribution of tools for compromising security such as but not limited to password guessing programs, cracking tools, packet sniffers or network probing tools.
	4.3 Unauthorised access to another user's electronic files, email or other electronic communication systems, use of another person account details either with or without their knowledge is not permitted.
	4.4 Any staff member, student or other person that successfully or unsuccessfully attempts to break password files will be in breach of this policy.

	4.5 Any communications which defames an individual, organisation, company or business.
	4.6 Any communication activities that are intended to bring the University or its officers into disrepute.
	4.7 Electronic communications can create binding legal commitments. System users are not permitted to authorise transactions or agreements except as provided in University procedures.
	4.8 The use of electronic communications for sending 'Junk mail', For-profit messages or chain letters is strictly prohibited.
	4.9 All e-mails sent externally from the University e-mail service may automatically have a notice attached to them to address electronic legal risks. This notice must not be altered or interfered with in any way, except by Authorised Persons. The use of this notice may not necessarily prevent the University or the sender of the e-mail from being held liable for its contents.
	4.10 Any communications which are likely to be contrary to the law must not be accessed or distributed and any conduct that breaches such laws may lead to criminal or civil proceedings and/or penalties for which they will be held personally accountable and/or result in discipline action up to and including termination of employment. This includes material which is in breach of legislation relating to defamation, racial vilification, pornographic, unlawful discrimination, harassment or online content and covered by legislation and guidelines as outlined below:
	4.10.1 Trade Marks Act 2000 (Amended) A user must not copy a trademark or logo belonging to another party. Trade mark infringement will expose the user to liability for damages.
	4.10.2 Trade Practices Users should not copy material from an external site onto a Swinburne website (including features such as logos and trademarks) so that persons accessing the website would believe that Swinburne had been authorised to carry the material. This would constitute passing off or deceptive or misleading conduct.
	4.10.3 Spam Users must not send unsolicited commercial electronic messages. Any commercial messages that are sent electronically (including email, instant messaging or telephone accounts) must include information about the individual or organisation who authorised the sending of the message and a functional unsubscribe facility.
	4.10.4 Anti-discrimination University IT facilities must not be used to humiliate, intimidate or offend others on the basis of their race, gender, or any other attribute. Electronic communications must not be used to publish, send or distribute material that is harassing, obscene or threatening, or material that may be considered unlawfully discriminatory, offensive or disruptive. This includes sexually oriented messages or images and sexual harassment messages. All users of electronic communications should be familiar with the University Anti-Discrimination and Harassment policy.
	4.10.5 Defamation Any communications which defames an individual, organisation, association, company or business. A user should not publish a statement about another person which could harm that other person's reputation. There is no need for the person to have been named specifically if he/she can reasonably be identified.

	<p>4.10.6 Illegal Content The University prohibit possession and use of certain kinds of online content, such as material depicting sex involving children. Illegal content is material which is offensive, morally improper and against current standards of acceptable behaviour. Please refer to Part 2 of the Malaysian Communications and Multimedia Content Code for details on the types of illegal content. A breach of this policy is a criminal offence prosecutable under Section 211 of the Communications and Multimedia Act 1998.</p>
	<p>4.10.7 Incitement to commit an offence Users must not publish material which is an incitement to commit or instruction in crime eg, material on how to prepare explosive devices, or how to steal or provide a link to a site that offers file-sharing software, use of which is likely to result in infringement of copyright.</p>
5.	Encryption/ Public Key Infrastructure
	All users of University e-mail and electronic communications are prohibited from using encryption devices, such as public key infrastructure, without approval of the Pro Vice-Chancellor and subject to the provision of encryption keys. All encryption keys will be provided to, and managed confidentially by, the Pro Vice-Chancellor or his/ her delegated officer.
6.	University Property
	6.1 The University is the owner of, and asserts copyright over, all electronic communications created by employees as part of their employment and sent through the University network.
	6.2 The University reserves the right to re-image its desktops and laptops as and when required.
	6.3 Staff, students and appointed persons that are provided with a desktop or laptop computer should not re-image to put personal photographs or images as Wallpaper or Screensavers that may cause offence or constitute harassment.
	6.4 Web Hosting
	6.4.1 All web-content that is hosted on University systems is to comply with the University style guide for content, and will identify the source of the publisher and the date of last up-date.
	6.4.2 All web-hosting services on University resources must be approved by the Pro Vice-Chancellor.
	6.4.3 The University will remove any material that is deemed to be offensive, indecent or inappropriate. This includes, but is not limited to obscene material, defamatory, fraudulent or deceptive statements, threatening, intimidating or harassing statements, or material that violates the privacy rights or property of others.
	6.5 Electronic communications created, sent or received by users over the University network are the property of the University, and may be accessed as records of evidence in case of an investigation. Electronic communications may also be subject to discovery in litigation and criminal investigations. For example, all information produced on computer, including emails, may be accessible for statutory compliance. Email messages can, and have been, retrieved from backup systems and organisations, their employees and the authors of email have been held liable for email messages that have been sent.

7.	Monitoring
	7.1 The University, with the concurrence of the Pro Vice-Chancellor, reserves the right to:
	7.1.1 Monitor or use any device or terminal without notice
	7.1.2 Inspect without notice any data on any resource owned by the University (regardless of data ownership), including electronic mail and other forms of communication.
	7.1.3 Capture and inspect any data in any networking infrastructure owned by the University.
	7.1.4 Delete or modify any data in any networking infrastructure in breach of this policy.
	7.2 Subject to clause 7.1.3, no University employee or student will be permitted to intercept, read, copy or modify electronic data (either in transit across a network or stored within a computer system) without the approval of the Pro Vice-Chancellor or delegate or consent of the addressee.
	7.3. The University will collect utilisation statistics based upon network address, network protocol and application use.
	7.4 The University may apply filtering systems to the University information systems. The filtering systems may limit use/activity through preventing the transmission of e-mail communications, either due to size or content.
	7.5 The University will establish processes to block access to World Wide Web site/ Internet sites that are deemed inappropriate and contrary to University policies and procedures.
	7.6 The University provides electronic communications on condition that users agree to monitoring occurring in accordance with this Policy. Use of electronic communications constitutes consent to monitoring in accordance with this Policy.
8.	<p>Copyright (Amended) Act (1997) Copyright material owned by third parties (such as computer programs, literary, dramatic, musical or artistic works, sound recordings, music recordings, cinematograph films, television or sound broadcasts, and published editions of works) including material in electronic form, must only be dealt with in accordance with the terms of the Copyright (Amended) Act 1997 and/or the terms of licence agreements entered into by the University.</p> <p>The Copyright (Amended) Act 1997 provides staff and students of the University with certain rights to use copyright material for the educational purposes of the University, or for the purposes of research and study and for some other purposes.</p> <p>Where staff and students do not have the right to use or deal with copyright material, copying or communicating such material may give rise to personal and/or University liability for copyright infringement and may result in personal liability for damages and in some cases for criminal sanctions.</p> <p>The University strongly supports the rights of copyright owners as set out in the Copyright (Amended) Act 1997 and will not tolerate reckless or deliberate infringement of those rights. The University also strongly supports the rights of copyright users as set out in the Act.</p> <p>The University takes very seriously the use of its network for infringement of copyright. Network users must not copy or communicate copyright materials unless with the permission of the copyright owner, or within the terms of the Copyright Act. Such</p>

	<p>infringement may occur by the use of email, file transfer, file sharing, provision of information via online systems, publication on the web, and other methods.</p> <p>In particular, the use of file-sharing software or other methods to obtain or provide infringing copies of music, movies or other copyright material is expressly forbidden, and is regarded as a serious offence.</p> <p>Where a copyright owner believes that the University network is being used to infringe his or her copyright, the university take-down procedure should be followed in order to report the infringement to the Manager, Information Resources so that action may be taken by the University. Where a user of the network is aware of a copyright infringement, this should be reported to the Manager, Information Resources.</p>
9.	Confidentiality
	9.1 While every attempt is made to ensure the security of the University's computer network, users must be aware that this security is not guaranteed, particularly when communicating with an external party.
	9.2 Users are required to control the use and release of personal information and restrict access to personal information in order to protect privacy. Collecting, using and disclosing personal information by e-mail may put the privacy of personal information at risk. Only the minimum amount of personal information necessary to accomplish the purpose for which it is required should be transferred by e-mail.
10.	Viruses
	10.1 Electronic Communications are potential delivery systems for computer viruses which have the potential to seriously damage the University network. All data, programs and files which are downloaded electronically or attached to messages should be run through a virus scan program before being launched, opened or accessed. In the event that a user receives a file that they suspect contains a virus it should be reported immediately to their line Manager (staff) or computer laboratory assistant/Manager (students).
11.	Attribution
	There is always a risk of false attribution of electronic communications. It is possible that communications may be modified to reflect a false message, sender or recipient. In these instances an individual may be unaware that he or she is communicating with an impostor or receiving fraudulent information. If at any stage if a user is concerned about the contents of a message received or the identity of the publisher of the electronic information, action should be taken to verify their identity by other means. If a user believes an electronic communication has been intercepted or modified, their Manager or computer laboratory assistant/Manager should be informed.
12.	Complaints
	<p>If a user of the University electronic communications network receives an internal or external Electronic Communication that is offensive or inappropriate, it should be raised with, in the case of staff members, their Head of Unit Manager or Human Resources if the Manager is the cause of the complaint or, in the case of students, the Manager, Information Technology Services.</p> <p>All allegations of breaches of privacy should be referred to the Manager, Information Technology Services.</p>

SECTION 3 - PROCEDURE

PROCEDURE

Not applicable.

SUPPORTING DOCUMENTATION

Forms and Records Management

Form	Retention Time	Retention Location
None		

Related Material

Name	Location	Document Type
Code of Conduct		Policy
General Misconduct		Policy
Anti-discrimination and Harassment		Policy
Information Technology Security		Policy
The Malaysian Communications and Multimedia Content Code	http://www.cmcf.org.my/code.asp	Guideline

SECTION 4 - GOVERNANCE

RESPONSIBILITY

Policy Owner	Manager, Information Technology Services
---------------------	--

VERSION CONTROL AND CHANGE HISTORY

Version Number	Approval Date	Approved by	Amendment
1	21 May 2009	Executive Committee	New policy; Previously used SUT Australia policy

POLICY & PROCEDURE DIRECTORY REQUIREMENTS

CATEGORY
University Management, Information Support Services

KEYWORDS
IT, Information technology, acceptable use, systems