

Policy and Procedure



SWINBURNE
UNIVERSITY OF
TECHNOLOGY

Name: IT Systems Acceptable Use

Approved by: Vice-Chancellor

Date approved: 24 August 2012

SECTION 1 – INTRODUCTION	2
PURPOSE.....	2
SCOPE.....	2
SECTION 2 – POLICY	3
PRINCIPLES.....	3
POLICY.....	3
SECTION 3 – PROCEDURE	9
PROCESS MAP	11
SECTION 4 – REFERENCE AND SUPPORTING INFORMATION	12
DEFINITIONS.....	12
SUPPORTING DOCUMENTATION.....	13
SECTION 5 – GOVERNANCE	14
RELATED EXTERNAL REFERENCES.....	14
RESPONSIBILITY.....	14
CHANGE HISTORY.....	15
RELATED SWINBURNE LEGISLATION AND POLICIES	16

SECTION 1 – INTRODUCTION

PURPOSE

This policy sets out the terms and conditions for the use of Swinburne University of Technology (hereafter referred to as “the University”) information technology network. This IT Systems Acceptable Use Policy and Procedure ensures the continued effective operation and support for the University’s academic, teaching, research and administrative operations as well as compliance with any rules or regulations under which the University is required to operate.

SCOPE

This policy applies to all Users of the University’s network as well as any computing equipment or other device connected to the University’s computer network irrespective of location or purpose. Use of the University information technology network includes all transmissions to or through the University network. This policy excludes Sarawak Campus.

The Information Technology Systems 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, data storage, computer accounts, software, software applications, telephony services and voicemail. Authentication and authorization policy and procedures apply to all production, development and test environments.

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.

The IT Systems Acceptable Use Policy and Procedure is committed to and guided by the principles of:

- maintaining a secure computing environment that supports the business needs of the University and is used primarily for University related activities
- providing access to computing infrastructure and electronic communications on condition that Users agree to act in accordance with this Policy
- ensuring that Users are aware of, understand and accept that
 - use of electronic communications constitutes consent to monitoring in accordance with this Policy.
 - breaches of this policy are regarded as a serious matter and the University may take action including revoking or restricting any right to use electronic communications, cautioning, or, in appropriate circumstances, formal action in accordance with University disciplinary policies and/or legal proceedings.
 - 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.

POLICY

1	Policy awareness
1.1	Policy Distribution
1.1.1	Users will be made aware of this policy prior to gaining access to Swinburne's computing environment.
2	Access and use
2.1	Authorised Access
2.1.1	The University permits the use of the University's information technology network through local or remote access by staff, affiliates and students who have valid accounts created and which uniquely identify the user of the account.
2.1.2	Users are responsible for all activities undertaken using their accounts.
2.1.3	Users must not share username and password with anyone else.
2.1.4	Users must not permit other persons to use their account.
2.1.5	Users must select passwords that follow the Password Guidelines contained in the IT Security Policy.
2.1.6	Users must log out or lock their computers whenever they are to be left unattended.
2.2	Authorised use
2.2.1	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: <ul style="list-style-type: none">▪ employees – their employment with the University

Please note: Printing this document may make it obsolete.

For the latest version of this policy always check the [Policies and Procedures Directory](#)

	<ul style="list-style-type: none"> ▪ 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>2.2.2 Except as provided for in 2.4, the network must:</p> <ul style="list-style-type: none"> ▪ only be used for University purposes ▪ where authorised or required by law ▪ with the express permission of an Authorised Person ▪ comply with any codes of conduct which apply to the User, such as the University Code of Conduct <p>2.2.3 The University requires staff and students use the wired network provided at the desktop, in the classroom and in student laboratories as the primary method for connecting to the University network.</p> <p>2.2.4 On-line conferences, discussion groups, email lists 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.</p> <p>2.2.5 Due to the evolving nature of social media, it is incumbent on all users to ensure that they familiarise themselves with the latest University Social Media Communications Guidelines and to act in accordance with these guidelines (and all other related University policies) when participating in social networking activities.</p> <p>2.2.6 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.</p> <p>2.2.7 Large downloads or transmissions should be minimised to ensure the performance of electronic communications by other users is not adversely affected.</p>
2.3	<p>Unauthorised access</p>
	<p>2.3.1 The following is not permitted:</p> <ul style="list-style-type: none"> ▪ use of another person's account details either with or without their knowledge ▪ unauthorised access to another person's electronic files, email or other electronic communications ▪ any attempt to circumvent the user authentication or security of any host, network or account
2.4	<p>Unauthorised use</p>
	<p>2.4.1 Unauthorised use includes those actions which are not within the boundaries of normal and appropriate practice which includes, but is not limited to:</p> <ul style="list-style-type: none"> ▪ unauthorised interception, reading, copying or modifying of electronic data on University information technology systems ▪ unauthorised access, creation, modification or deletion of University records including: <ul style="list-style-type: none"> ○ student records ○ human resource records ○ payroll records ○ financial records ○ library systems ○ any other University electronic system ▪ the distribution, use or attempted use of tools for compromising security such as but not limited to: <ul style="list-style-type: none"> ○ password guessing programs ○ cracking tools ○ packet sniffers

	<ul style="list-style-type: none"> ○ network probing tools ▪ installation or use of unauthorised software on computers connected to the Swinburne network
	<p>2.4.2 The University's network must not be used for communications that:</p> <ul style="list-style-type: none"> ▪ defame an individual, organisation, association, company or business ▪ bring the University or its officers into disrepute ▪ relate to sending 'junk mail', for-profit messages, or chain letters <p>2.4.3 The University's network must not be used to attack/hack any systems.</p> <p>2.4.4 The use of Peer to Peer software is not permitted without the prior written approval of the Chief Information Officer.</p>
2.5	<p>Illegal use</p> <p>2.5.1 Any communications that are likely to be contrary to applicable laws must not be accessed or distributed. This includes, but is not limited to, material that is in breach of legislation relating to defamation, racial vilification, pornography, discrimination, harassment or online/other content.</p>
2.6	<p>Personal use</p> <p>2.6.1 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 breach of this policy.</p> <p>2.6.2 Subject to limited personal use provisions of this policy, electronic communications must not be used to access inappropriate material, conduct private business or private commercial transactions, gamble, or carry out excessive and regular research into non-work related topics.</p>
3	Data ownership
3.1	<p>Ownership of data and records</p> <p>3.1.1 Subject to the University's statutes and regulations, the University is the owner of, and asserts copyright over, all electronic communications created by employees as part of their employment.</p> <p>3.1.2 Subject to the University's statutes and regulations, 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 an investigation or in response to other actions such as audit, litigation, criminal investigations or Freedom of Information requests.</p>
3.2	<p>Data encryption</p> <p>3.2.1 All users of University e-mail and electronic communications are prohibited from using encryption mechanisms, such as public key infrastructure, without approval of the Chief Information Officer. Approval will only be given subject to the provision of encryption keys and all encryption keys must be provided to, and managed confidentially by, the Chief Information Officer or his/her delegated officer.</p>
4	Information security
4.1	<p>Account security</p> <p>4.1.1 Users must take reasonable steps to ensure their accounts remain secure.</p>
4.2	<p>Email and electronic communications</p> <p>4.2.1 Email is an official method of communication to University staff. Mass electronic communications, official or otherwise, should only be sent in accordance with related University policies. Staff should not disable the receiving of official mail.</p> <p>4.2.2 Staff must use the official Swinburne email system and email address only. The standard format of all staff addresses is firstinitialsurname@swin.edu.au</p>

	<p>4.2.3 Staff are not permitted to forward or redirect their University email account to a third party email system.</p> <p>4.2.4 Where there is a University system provided for a specific purpose, it is not permitted to establish another system for the same purpose.</p> <p>4.2.5 Users must be aware that while every attempt is made to ensure the security of the University's computer network, electronic communications (especially email), cannot be guaranteed secure. As such, users are advised to exercise caution, (particularly when communicating with parties external to the University) in the use of electronic communications for sending confidential information.</p> <p>4.2.6 Any email sent externally by staff to non-Swinburne email addresses will automatically have a legal disclaimer notice attached to them. 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 email from being held liable for its contents.</p> <p>4.2.7 Users are advised that there is always a risk of false attribution of electronic communications and that at any time it is possible that communications may be modified to reflect a false message, sender or recipient. In such cases users may be unaware that they are communicating with an impostor or receiving fraudulent information. If at any stage 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 and the service desk or in the case of students, the service desk should be informed.</p>
4.3	<p>Application system security</p> <p>4.3.1 Authentication</p> <p>4.3.1.1 Software applications that require different levels of access for different users must have a method of secure authentication.</p> <p>4.3.2 Authorisation</p> <p>4.3.2.1 In all cases any changes to application authorisation levels will need to be approved by the business owner.</p> <p>4.3.2.2 Accounts with full administrative access to servers such as root or admin will only be granted to relevant ITS infrastructure staff.</p> <p>4.3.2.3 Database accounts with system privileges will only be granted to ITS information systems database administrators.</p> <p>4.3.2.4 Access to test and development systems will be governed by the same rules as production systems.</p> <p>4.3.3 Application administrator access</p> <p>4.3.3.1 The Application administrator will be granted an account within the Application with administrator access so that they can manage all aspects of the Application including assigning further authorisation levels.</p> <p>4.3.3.2 The Application administrator account will not have administrator access to the server itself.</p>
4.4	<p>Confidentiality</p> <p>4.4.1 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.</p>

4.5	<p>Viruses</p> <p>4.5.1 Electronic communications are potential delivery systems for computer viruses which could seriously damage the University's network. All data, programs and files that are downloaded electronically or attached to messages should be run through a virus scan program before being launched, opened or accessed.</p> <p>In the event that a user receives a file that they suspect contains a virus it should be reported immediately to the service desk.</p> <p>4.6 External hosting</p> <p>4.6.1 Written approval must be obtained from the Chief Information Officer prior to establishing any internet hosting or services external to the University.</p>
<p>5</p> <p>5.1</p> <p>5.2</p>	<p>Monitoring and filtering</p> <p>5.1.1 The University will collect utilisation statistics based upon network address, network protocol application use or user-based.</p> <p>5.1.2 Subject to the approval of the Vice-Chancellor or delegate, the University reserves the right to (without notice):</p> <ul style="list-style-type: none"> ▪ monitor the use of any device or terminal ▪ inspect any data residing on any University-owned resource (regardless of data ownership), including electronic mail and other forms of communication ▪ capture and inspect any data in any computing infrastructure owned by the University ▪ delete or modify any data in any networking infrastructure in breach of this policy ▪ re-image its desktops and laptops as and when required <p>5.1.3 Users must not intercept, read, copy or modify electronic data (either in transit across a network or stored within a computer system) without the approval of the Vice-Chancellor or delegate or consent of the addressee.</p> <p>5.2 Filtering</p> <p>5.2.1 The University may apply filtering systems to the University network that limit use/activity by preventing communications based on size or content.</p> <p>5.2.2 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.</p> <p>The University will remove any material that is deemed to be offensive, indecent or inappropriate</p> <p>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.</p>
<p>6</p> <p>6.1</p>	<p>Non-compliance</p> <p>6.1.1 Failure to comply with this Policy by a staff member will be referred to the Director, Human Resources and/or Head of Management Unit and dealt with in accordance with processes in relation to misconduct or unsatisfactory performance (whichever is applicable).</p> <p>6.1.2 Failure to comply with this Policy by non-employees e.g. a contractor or casual staff member will be referred to the Head of Management Unit and dealt with in accordance with the relevant processes.</p> <p>6.1.3 Failure to comply with the Policy by a student will be dealt with in accordance with University statutes and regulations dealing with student discipline.</p> <p>6.1.4 Conduct that breaches laws will be referred to the relevant legal body and, in addition</p>

	to any disciplinary action by the University, may lead to criminal or civil proceedings and/or penalties for which the User will be held personally accountable.
6.2	<p>Complaints</p> <p>6.2.1 Users who receive an internal or external electronic communication that is offensive or inappropriate, should in the case of staff members, raise it with their head of management unit (or if the manager is the cause of the complaint) with Human Resources, or in the case of students, with the Director, Student Operations.</p>

SECTION 3 – PROCEDURE

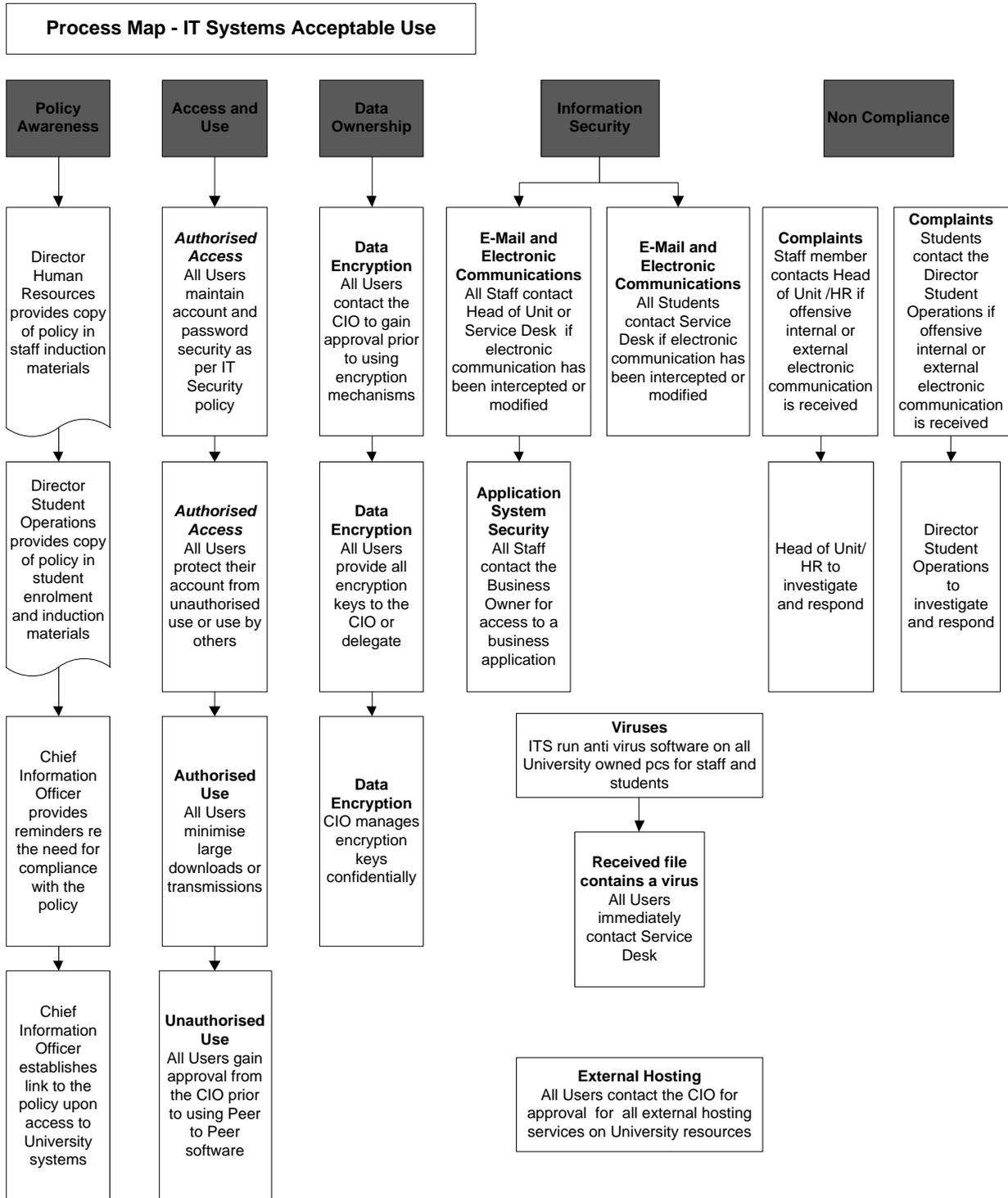
Procedure steps		Responsibility
1	Policy awareness	
1.1	Policy distribution	
	1.1.1 Provide a copy of the policy in staff induction materials.	Director Human Resources
	1.1.2 Provide a copy of the policy in student enrolment and induction materials.	Director Student Operations
	1.1.3 Provide regular and timely reminders of the need for compliance with the policy.	Chief Information Officer
	1.1.4 Establish a link to the policy upon access to the University systems.	Chief Information Officer
2	Access and use	
2.1	Authorised access	
	2.1.1 Maintain account and password security standards as outlined in the Information Technology Security Policy	All users
	2.1.2 Take all reasonable precautions to protect the account from unauthorised use or use by others.	All users
2.2	Authorised use	
	2.2.1 Take all reasonable steps to minimise large downloads or transmissions.	All users
2.3	Unauthorised use	
	2.3.1 Contact the Chief Information Officer to gain approval prior to using Peer to Peer software. Permission will only be given in exceptional circumstances.	All users
3	Data ownership	
3.1	Data encryption	
	3.1.1 Contact the Chief Information Officer to gain approval prior to using encryption mechanisms. Approval will only be given subject to the provision of encryption keys.	All users
	3.1.2 Provide all encryption keys to the Chief Information Officer or his/her delegate.	All users
	3.1.3 Manage encryption keys confidentially.	Chief Information Officer
4	Information security	
4.1	Email and electronic communications	
	4.1.1 Contact the Head of Unit Manager and the Service Desk if you believe that an electronic communication has been intercepted or modified.	All staff
	4.1.2 Contact the Service Desk if you believe that an electronic communication has been intercepted or modified.	All students
4.2	Application system security	

Please note: Printing this document may make it obsolete.

For the latest version of this policy always check the [Policies and Procedures Directory](#)

4.3	<p>4.2.1 Contact the Business Owner to obtain access, increase levels of access and gain authorisation to use a particular business Application.</p> <p>Viruses</p> <p>4.3.1 Automatically run antivirus software on all University-owned pcs for staff and students.</p> <p>4.3.2 Immediately Contact the Service Desk if a received file contains a virus.</p>	<p>All staff</p> <p>ITS</p> <p>All users</p>
4.4	<p>External hosting</p> <p>4.4.1 Contact the Chief Information Officer to gain approval for all external hosting services on University resources.</p>	<p>All users</p>
5	Non-compliance	
5.1	<p>Complaints</p> <p>5.1.1 Contact the head of management unit (or if the manager is the cause of the complaint), Human Resources if an internal or external electronic communication is received that is offensive or inappropriate.</p> <p>5.1.2 Investigate and respond to staff member's complaint</p> <p>5.1.3 Contact the Director, Student Operations if an internal or external electronic communication is received that is offensive or inappropriate.</p> <p>5.1.4 Investigate and respond to student's complaint</p>	<p>All staff</p> <p>HMU/HR</p> <p>All students</p> <p>Director Student Operations</p>

PROCESS MAP



Please note: Printing this document may make it obsolete.
 For the latest version of this policy always check the [Policies and Procedures Directory](#)

SECTION 4 – REFERENCE AND SUPPORTING INFORMATION

DEFINITIONS

Word/Term	Definition
Application or Information System	Any IT based system, data or process used to support the business operations of the organisation
Authentication	A process of verifying and validating an individual is who they claim to be
Authorisation	The process of assigning levels of access to individuals who have been authenticated.
Authorised person	A person authorised by the Vice-Chancellor.
Business Owner	<p>An appropriate representative of the Swinburne User community responsible for the processes and policies relating to the use of, and integrity of data within an Application. The Business Owner is also responsible for ensuring that Application changes are justified and will not compromise any business processes and/or IT product dependent on that Application.</p> <p>While responsibilities are assigned to this position, a Business Owner may formally delegate some of these responsibilities to appropriate staff in their business unit.</p>
Confidential Information	Includes information that would reasonably be understood to be confidential in nature. This includes but is not limited to Personal Information, Sensitive Information, commercial-in-confidence information or information that has been identified by its provider as being confidential.
Directory	A system containing User Account information (including User IDs and Passwords) that may be used by applications to support Authentication and Authorisation processes.
Electronic communications	Includes but is not limited to publishing and browsing on the Internet, electronic mail (email), electronic bulletin/notice boards, electronic discussion/news groups, file transfer, file storage, video conferencing, streaming media, instant messaging, “chat” facilities, social networking provision of information via online systems, online subject delivery systems, VoIP telephones and network devices.
Network	Swinburne’s data and telecommunications network infrastructure.
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
Personal Information	Information designated as Personal Information in accordance with the University’s Privacy policy
Sensitive Information	Information designated as Sensitive Information in accordance with the University’s Privacy policy
SIMS	Swinburne Identity Management System
Social Media	Any form of media generally found on online social networking websites

Please note: Printing this document may make it obsolete.

For the latest version of this policy always check the [Policies and Procedures Directory](#)

Staff	Any person employed by the University
User	Any person using Swinburne's network or computing environment.
User Account	A computer account, specific to a user, that gives access to certain system resources such as data storage, printing and network services (e-mail, etc.) Access to this account is secured by a User ID and Password.
User ID	The User-ID is a unique alphanumeric string allocated by the system administrator and used to identify a computer system User.
VPN	Virtual Private Network

SUPPORTING DOCUMENTATION

Anti-Discrimination Policy and Procedure
Code of Conduct Policy and Procedure
Copyright Policy and Procedure
Electronic Data Storage and Backup
General Misconduct Policy and Procedure
Information Technology Security Policy and Procedure
Management of University Records and Freedom of Information Policy and Procedure
Official Email
Password Guidelines
Privacy Policy and Procedure
Sexual Harassment Policy and Procedure
Social Media Communications Guidelines
Social Media Users Guide
Student General Misconduct Regulations
Student Misconduct Policy and Procedure
Swinburne University of Technology, Academic and General Staff Certified Agreement 2009
Unsatisfactory Work Performance/Conduct – Academic and General Staff
Unsatisfactory Work Performance/Conduct – TAFE Teachers
Student Electronic Communications
Victorian TAFE Teaching Staff Multi-Business Agreement 2009

SECTION 5 – GOVERNANCE

RELATED EXTERNAL REFERENCES

Name	Link
AARNet	http://www.aarnet.edu.au/about-us/policies.aspx
Competition and Consumer Act 2010 (formerly Trade Practices Act 1974) (Cth)	http://www.comlaw.gov.au/Details/C2011C00003/
Copyright Act 1968 (Cth)	http://www.comlaw.gov.au/Series/C2004A07378
Privacy Act 1988 (Cth)	http://www.comlaw.gov.au/Details/C2011C00179
Spam Act 2003 (Cth)	http://www.austlii.edu.au/au/legis/cth/consol_act/sa200366/
The Disability Discrimination Act 1992 (Cth)	http://www.austlii.edu.au/au/legis/cth/consol_act/dda1992264/
The Equal Opportunity Act 1995 (Vic)	http://www.austlii.edu.au/au/legis/vic/consol_act/EOA1995250/
The Human Rights and Equal Opportunity Commission Act 1986 (Cth)	http://www.austlii.edu.au/au/legis/cth/consol_act/hraeocpaaa19861054/
The Racial Discrimination Act 1975 (Cth)	http://www.austlii.edu.au/au/legis/cth/consol_act/rda1975202/
The Racial Hatred Act 1995 (Cth)	http://www.austlii.edu.au/au/legis/cth/num_act/rha1995109/
The Sex Discrimination Act 1984 (Cth)	http://www.austlii.edu.au/au/legis/cth/consol_act/sda1984209/

RESPONSIBILITY

Responsible manager(s)	Vice-Chancellor, Vice-President (Student and Corporate Services)
Policy administrator	Chief Information Officer and Director, Information Technology Services
Approving body	Vice-Chancellor

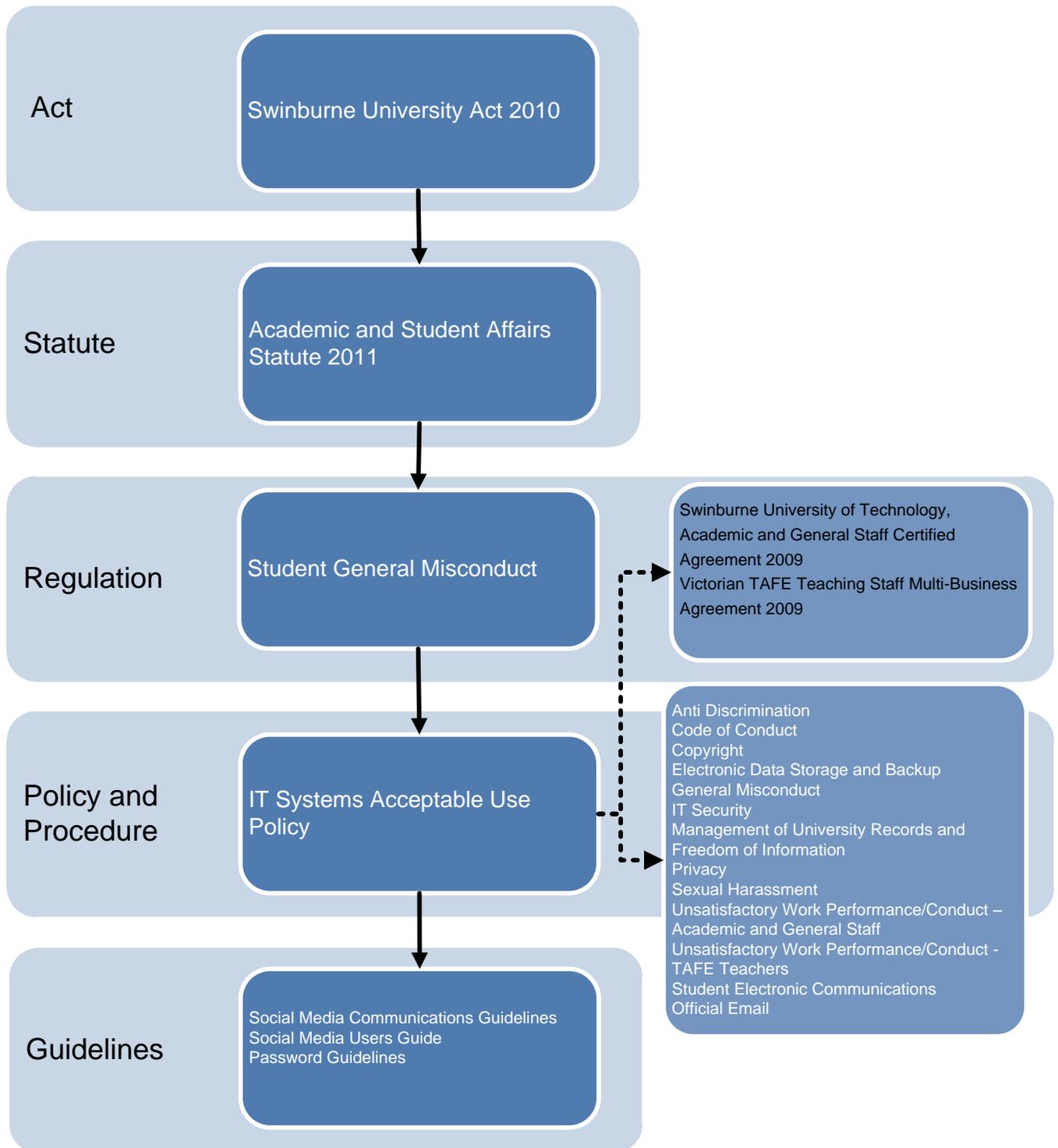
CHANGE HISTORY

Version	Approval date	Approved by	Change
1	7 November 2003	Vice President (Resources) and Information Management Committee	Previously known as Information Technology Systems Access and Use Policy
2	6 September 2005	Executive Group	
3	24 August 2012	Vice Chancellor	Rewritten in new format

RELATED SWINBURNE LEGISLATION AND POLICIES

This policy and procedure supports the Swinburne Student General Misconduct Regulations 2012 and should be read in conjunction with related internal and external legislation and relevant management guidelines.

In cases where the policy and procedure or guidelines conflict with the Student General Misconduct Regulations 2012, or related legislation, the regulations and related legislation always take precedence.



Please note: Printing this document may make it obsolete.
For the latest version of this policy always check the [Policies and Procedures Directory](#)