

IT001 INFORMATION TECHNOLOGY

1. Purpose

IT resources are essential for accomplishing SAIBT's mission of pursuing excellence in teaching and learning. Members of SAIBT's community are granted shared access to SAIBT's IT resources, and these must be used and managed responsibly to ensure their integrity, security and availability for appropriate educational and business activities.

This policy applies irrespective of where the IT resources are accessed and used, and applies to all users of SAIBT's IT resources, including those who install, develop, maintain, administer and use those systems and applications.

2. Definitions

- 'user' and 'users' referred to herein includes SAIBT staff and other authorised users of SAIBT's IT resources.
- IT resources includes all computers, electronic communication devices and software owned or leased by SAIBT, and network facilities which link computers within SAIBT and which provide external access such as the Internet.

3. Responsibilities

It will be the user's responsibility to become familiar with the rules governing use of SAIBT's IT resources.

Users who are authorised to permit other persons to use SAIBT's IT resources must ensure that those persons are made aware of the rules governing the use of SAIBT's IT resources, and should have them sign a written acknowledge that they will observe the rules.

Users learning of any violation the rules must bring the matter to the attention of an appropriate officer (eg Academic Director, lecturer, IT staff) without delay.

4. Authorisation

The user may only make use of equipment, networks or information for which proper authorisation has been given. In the case of staff, authorisation must be obtained from the person or unit responsible for the facility (e.g. Director, Operations or nominee). In the case of students, authorisation occurs automatically upon enrolment at SAIBT.

The user are responsible for ensuring that passwords, accounts, software and data are adequately secured. The user will be held responsible for all activities, which originate from their account. It is in everyone's interest that secure password is selected.

If the user knows or suspects that another person has gained unauthorised access to their account, they must notify the IT Manager on 8302 1571.

The user must not use any means, electronic or otherwise, to discover others' passwords.

Students are permitted only to use resources available within the SAIBT computer labs. Under no circumstances are students permitted to use staff or sessional staff machines. However, temporary authorisation may be granted only with constant and direct supervision by a person able to give authorisation (e.g. Academic Director or nominee). Sessional staff are permitted to use

resources in the computer labs and in the sessional area/s. Full time staff are permitted to use any and all resources.

3. Responsible use of Resources

3.1 Internet and email services can only be used for:

- SAIBT purposes – ie any activity conducted for purposes of accomplishing SAIBT business related to research, teaching and learning, course of study, administrative activities, and professional development
- Limited personal use’ – ie use that is infrequent and brief. This use should generally occur during personal time and should not include uses that:
 - require substantial expenditure of time
 - are for private business, personal gain or profit
 - support political campaigns, candidates, legislation or ballot issues
 - impede the efficiency of intranet, internet or email services
 - clog mailboxes with large numbers of messages
 - waste SAIBT resources, such as playing games
 - would violate or breach SAIBT’s Code of Conduct, any State or Federal legislation, or any SAIBT policy or regulation, or harm SAIBT’s image and reputation

3.2 As a guide, use that occurs more than a few times per day and/or periods longer than a few minutes would not be considered limited personal use.

3.3 The user should use SAIBT electronic mailing lists for SAIBT purposes only. It is inappropriate to:

- Mass email messages of a commercial, political, lobbying or fundraising nature
- Forward chain letters or electronic “petitions”, or to ask recipients to forward messages
- Send anonymous mailings
- Solicit support (financial or otherwise) for charity, or special causes not connected with a SAIBT effort
- Send unverified public service announcements (such as virus alerts, unsafe products, lost and found etc.)

3.4 A message sent to a SAIBT electronic mailing list must be relevant to the membership of the list.

3.5 The user should not use the SAIBT network, whether at an Institute site or another site including at home, to access inappropriate Internet sites.

Inappropriate Internet sites include but are not limited to:

- o Sites that are illegal or hold illegal content
- o Sites that are pornographic or contain inappropriate sexual material
- o Sites that advocate hate or violence

- o Sites that offer games or software that are unrelated to academic programs

3.6 The user must not download, distribute, store or display offensive or pornographic graphics, images or statements or other material obtained from inappropriate Internet sites.

3.7 The user must not download, distribute, store or display material that could cause offence to others, for example offensive material based on gender, ethnicity and political beliefs.

3.8 The user must not attempt to email “spoof” i.e., construct electronic communication so it appears to be from someone else.

3.9 Where you are representing the views of the Institute, the communication must identify your position within the Institute. Where the view expressed is the ‘official’ Institute view, the authorised source and author of that view should be identified.

3.10 The user must not express views on behalf of the Institute without official authorisation to do so, or to allow another person to reasonably misconstrue that a personal view represents the official position of the Institute. In circumstances where readers might reasonably conclude a personal view is representative of the Institute, the user must clearly state that the opinion expressed is that of the writer, and not necessarily that of the Institute, or words to that effect.

3.11 The Institute’s logos and designs are the property of the Institute and may only be used for approved Institute documents.

3.12 The user must take reasonable steps to ensure physical protection including damage from improper use, food and drink spillage, electrical power management, anti-static measures, protection from theft, and sound magnetic media practices.

3.13 Ensure computers are not left unattended without first logging-out and/or securing the entrance to the work area – particularly if the computer system to which they are connected contains sensitive or valuable information.

3.14 The user must not install software or hardware, or change the standard PC configuration in any way without the express permission of the SAIBT IT Manager, or authorised nominee.

1. Respect for other users of Resources

Successful use of Institute information technology resources depends upon a spirit of mutual respect and co-operation to ensure that everyone has equitable privileges, privacy and protection from interference or harassment.

To this end:

4.1 The user must respect the privacy of other users and thus not intentionally seek information on, obtain copies of, or modify files, tapes, passwords or any type of data belonging to other users unless specifically authorised to do so.

4.2 The user must not intentionally disrupt or damage the academic, research, administrative, or related pursuits of others.

4.3 The user must not use e-mail, discussion forums or web pages under your control, to provide or communicate obscene materials, or that threatens, harasses, intimidates or singles out individuals or groups for degradation or harassment in violation of Federal or State law, and other Institute policies and regulations.

4.4 The user must not display on screens images, sounds or messages, which could create an atmosphere of discomfort or harassment to others.

4.5 The user must not knowingly create or propagate a virus, worm or any other form of malicious software.

4.6 The user must not tamper with hardware components or hardware configurations without the express permission of the person/s responsible for that particular item of equipment.

This includes:

- o Workstation, monitor, keyboard and mouse
- o Printers and other peripherals
- o Network outlets, cabling and other components
- o Phones
- o Any part of a lab or any other installation used by the general population of the Institute

4.7 The user must respect the integrity of the system and not use Institute resources to develop or execute programs that could infiltrate the system, tamper with or attempt to subvert security provisions, or damage or alter the software components of the system. This also applies to systems maintained by others outside of SAIBT that you access electronically or physically.

5. Privacy

The Institute's network, systems and facilities are the property of the Institute. Anything sent or received using the network; systems and facilities of the Institute will therefore be transmitted and stored on Institute property.

Accordingly it is likely to be reviewed by the Institute. This applies whether you use the Institute resources at an Institute site, at home, or any other location.

5.1 The Institute therefore reserves the right to monitor both usage and content of email messages, discussion forums and visits to Internet sites using Institute resources to:

- o Identify appropriate use
- o Protect system security
- o Maintain system performance
- o Protect the rights and property of the Institute
- o Determine compliance with policy and State and Federal legislation

5.2 The Institute also monitors and records network traffic including:

- o Email and internet sites accessed
- o Usage data such as account names, source and destination accounts and sizes
- o Dates and times of transmission or access
- o Size of transmitted material
- o Other usage related data

This information is used for accounting purposes, troubleshooting and systems management.

5.3 The Institute reserves the right to inspect, copy, store and disclose the contents of the electronic communications of its employees and other authorised users (e.g. students), for the purposes of identifying inappropriate use, upon receiving a complain, investigation request or allegation of misuse, and following authorisation from appropriate SAIBT managers, the Police or other law enforcement agencies to assist in the investigation of an offence. The contents of electronic communications, properly obtained for legitimate business purposes, may be disclosed without permission of the employee or authorised user.

5.4 Monitoring and inspection can apply to personal and business use of intranet or Internet services and personal and business related email messages.

5.5 The user should always assume that everything sent by e-mail is totally public and might be read by people other than expected recipients. Any email messages, whether personal or business, may be accessed as 'documents' under the Freedom of Information Act and may also be tendered in court as evidence.

The user should always assume that any web site visited will at least know the Internet address they are coming from and that the same is true for sent e-mail.

1. Copyright Compliance

1.1 The Copyright Act sets out the exclusive rights of copyright owners and the rights of users. In addition, certain uses may be covered by licence agreements to which the Institute is party. Full information is available in the SAIBT Copyright Guide.

6.2 It is illegal to place on a Web page any pictures or videos of people without the permission of the people in the picture or video and/or the copyright owner.

6.3 Software programs are protected by the Copyright Act. The user does not have the right to make and distribute copies of programs without specific permission of the copyright holder.

7. Breach of responsibly

7.1 The Institute considers any breach of the user's responsibilities to be a serious offence and reserves the right to copy and examine files or information resident on or transmitted via Institute information technology resources. Students deemed to be in breach of the above principles or guidelines are subject to disciplinary action, which may include suspension or expulsion. Staff deemed to be in breach of these principles or guidelines are subject to disciplinary action available under industrial provisions. Offenders may also be prosecuted under State, Federal and International laws.

7.2 The SAIBT IT Manager may temporarily remove material from web sites or close any account that is endangering the running of the system or that is being reviewed for inappropriate or illegal use.

Associated Policies and Legislation ***Racial Discrimination Act (Cwlth) 1975***
<http://scaleplus.law.gov.au/html/pasteact/0/47/top.htm>
(including

Guidelines and Procedures) ***Sex Discrimination Act (Cwlth) 1984 1975***
<http://scaleplus.law.gov.au/html/pasteact/0/171/top.htm>

Telecommunications Act

Trade Marks Act (1955) (Commonwealth)

Trade Practices Act (1974) (Commonwealth)