

# Student IT Acceptable Use Policy

---

## 1. Purpose

This policy informs all SIBT users of IT resources of their rights and responsibilities at all times, including use of the Navitas networks and wireless internet access, email, desktop, laptop and tablet computers, software and peripherals, and personally-owned equipment when it is connected to a Navitas network. In addition, Navitas staff are subject to the *Navitas IT Acceptable Use Policy* and *Navitas IT Acceptable Usage Policy Agreement* (see “Related Documents”).

## 2. Application

Information Technology (IT) is imperative to the teaching, communication, research and core business activities of SIBT. In recognition of this, Navitas provides access to IT resources to its users for teaching, research, administration and other specifically authorised purposes (see “Definitions”).

The computers and computer network at SIBT together with access to the internet and email are provided primarily for educational, professional and business purposes. The use of these facilities should therefore be consistent with that purpose.

## 3. Underlying Principles

SIBT takes the security of data, IT resources and infrastructure very seriously. Users must adhere to all elements of this policy. The principles of behaviour relating to the use of SIBT IT resources include:

- Respect for the law;
- Respect for other people; and
- Respect of the SIBT’s mission and values.

## 4. Acceptable Use Principles

### 4.1 *User Accounts*

Users are ultimately accountable for all actions attributed to their User Account.

To support this Users are responsible for safeguarding their passwords and/or other sensitive access control information related to their accounts or network access.

Users must not share their accounts, nor grant accounts to others nor otherwise extend their own authorised computer and network access privileges to others.

Users must not obtain nor attempt to obtain any electronic communication or information not intended for them.

Unattended work stations must always be logged off or left in the Workstation Locked mode (Ctrl + Alt + Delete) when the operator leaves their workstation unattended.

Students who withdraw or complete their studies will have their user account access terminated within three months of when their status is changed to Deferred, Terminated, Graduated or Withdrawn.

SIBT reserves the right to discontinue or vary user accounts at any time without notice. Where users are considered to be in breach of academic policies, matters may be subject to termination and disciplinary action. Serious breaches may involve permanent expulsion from SIBT and, in cases of suspected criminal activity, may involve referral of the matter to the relevant law enforcement authority(s) for criminal prosecution and other legal action to cover civil damages and penalties.

#### 4.2 *IT Systems Use*

Users may not use SIBT systems for any of the following activities:

- Gambling or any form of Internet gaming.
- Use any SIBT IT systems for personal financial gain, solicitation or private business purposes.
- Posting any SIBT Information to Internet bulletin boards, discussion lists, news groups, chat groups or other internet discussion forums that are accessible by the public

#### 4.3 *Safe Practices*

Users shall work in accordance with safe computing practices to minimise the risks associated with computer viruses.

While IT will make every effort to ensure the availability and integrity of IT resources, it cannot guarantee that they will always be available and/or free of any defects including malicious software such as computer viruses, the wilful introduction of computer viruses or other disruptive/destructive programs into SIBT.

If a user receives a suspected virus email or virus warning via the antivirus software application, they should notify IT immediately.

#### 4.4 *Inappropriate Material*

Users must not access, create, download, print, store, forward or send inappropriate content. Examples of which include, but are not limited to:

- Information or images containing indecent material (this includes pornographic or other sexually explicit material), or other material, which explicitly or implicitly refers to sexual conduct or preference.
- Information or images containing profane or abusive language. This includes anything that refers to or supports discrimination of any kind.
- Unwelcome propositions.
- Any defamatory, illegal, offensive, annoying or harassing material.
- Information intended to incite criminal activities or instructs others how to commit such acts.

Please refer to Appendix 1 Student Guide: Netiquette

#### 4.5 *Email*

Users must not make sure of SIBT resources to forward chain letters or spam mail, alter messages so they appear to have been sent by someone else, or delete/edit the automatic signature that appears on the bottom of SIBT emails.

At any stage if a user has a concern with 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, your manager should be informed.

#### 4.6 *Monitoring*

SIBT reserves the right to regularly audit IT systems to ensure compliance with this policy.

As part of normal system operation, SIBT reserves the right to maintain logs of email system activity. These logs identify sender, recipient, message size, relay, date and time.

All files, including those generated via internet email and proprietary email systems, are generally accessible by persons with system administration privileges (eg, SIBT IT Support staff). Users are discouraged from maintaining anything private on the email mailboxes.

Access to SIBT IT systems is provided to you on condition that you consent to monitoring in accordance with this and the IT Security Policy. Your use of SIBT IT systems constitutes your consent to the monitoring.

#### 4.7 *SIBT Assets*

Hardware always remains the property of the SIBT, on cessation of enrolment all SIBT hardware must be returned in a clean, tidy, working and prompt fashion to SIBT.

SIBT tablets, mobile devices, notebooks, laptops and desktop computers are issued for uses teaching and learning needs only. Any such device is not provided for non SIBT students to use (ie, friends, family, etc).

The unauthorised duplication of copyrighted computer software violates the law and is contrary to SIBT's standards of conduct and business practice. SIBT will comply with all licensing terms and conditions regulating the use of any software it acquires.

All requests for software and app licencing and purchases (including specialised software and apps) must go through the IT Department. This is to ensure:

- That apps and software are correctly assigned an asset number upon purchase and receipt.
- That apps and software are managed according to the correct version and licensing by the (Mobile) Device Management platform in use at SIBT
- That audits of apps and software on devices can occur against a reliable account of owned software.
- That upgrades of apps and software can occur, generally business wide, to ensure minimum confusion between versions.
- That all instances of licence documentation, software media and copies of delegation/invoice details for the software are held and accounted for by SIBT.

Software and apps and device licences always remain the property of SIBT, on cessation of a student's enrolment all SIBT software must be returned.

Student's are not permitted to install their own software on any SIBT computers, mobile devices, tablets, laptops or workstations, without prior approval from the IT Department. Failure to comply may result in users being held personally responsible for any data loss or penalties imposed for breach of copyright.

Installation or use of peer to peer file sharing programs by student's is not permitted on computers or devices connected to the SIBT network.

Student's shall not download or authorise downloading of information or software from the internet or emails to provide to a third party violate copyright, license agreements or contract of usage.

#### 4.8 *Breaches*

Any security exposures, misuse or non-compliance must be reported as soon as an occurrence is identified to IT Support or a Lab Demonstrator.

Failure to comply with this policy may result in any or all of the following:

- Suspension and/or termination of access to SIBT systems.
- Additional disciplinary action as determined by relevant Managers in line with existing policies.

#### 4.9 *Legal Requirements*

For legal purposes, mobile and messaging applications and email have the same standing in court as paper documents. Users must be aware that SIBT can be involved in litigation. Any records relating to use and activities in relation to mobile, messaging applications email, internet and intranet are discoverable by way of court order or subpoena. These include matters affecting legal proceedings, affecting personal affairs of users, parents, students, or third parties, as well as relating to research, or other communications even if communicated in confidence.

Email residing on or transmitted across SIBT systems is the property of SIBT. All electronic files are the property of SIBT, and users should act on the basis that they can be, and where necessary will be, held accountable for their messages and their stored files.

Should access to an individual's messaging logs, emails, files or internet logs be necessary for an alleged criminal offence or serious disciplinary matter the individual concerned will generally first be told the circumstances of the complaint and be present when the files or logs are opened. Notwithstanding the above, SIBT reserves the right for any reason whatsoever to inspect without forewarning any files or logs held on any SIBT computer.

#### 4.10 *Relevant Legislation*

Users need to be aware that certain conduct may breach laws outside of SIBT and lead to criminal or civil proceedings and/or penalties for which they will be held personally accountable. In Australia these laws include:

- Sex Discrimination Act 1984 (Cth) [http://www.austlii.edu.au/au/legis/cth/consol\\_act/sda1984209/](http://www.austlii.edu.au/au/legis/cth/consol_act/sda1984209/)
- Disability Discrimination Act 1992 (Cth) [http://www.austlii.edu.au/au/legis/cth/consol\\_act/dda1992264/](http://www.austlii.edu.au/au/legis/cth/consol_act/dda1992264/)
- Racial Discrimination Act 1975 (Cth) [http://www.austlii.edu.au/au/legis/cth/consol\\_act/rda1975202/](http://www.austlii.edu.au/au/legis/cth/consol_act/rda1975202/)
- Copyright Act 1968 (Cth) [http://www.austlii.edu.au/au/legis/cth/consol\\_act/ca1968133/](http://www.austlii.edu.au/au/legis/cth/consol_act/ca1968133/)
- Privacy Act 1988 (Cth) [http://www.austlii.edu.au/au/legis/cth/consol\\_act/pa1988108/](http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/)
- SPAM Act 2003 (Cth) [http://www.austlii.edu.au/au/legis/cth/consol\\_act/sa200366/index.html](http://www.austlii.edu.au/au/legis/cth/consol_act/sa200366/index.html) and
- Other relevant Commonwealth and/or State laws such as those relating to the transmission of offensive material and Telecommunications.

## 5. Definitions

**User** – for the purposes of this IT Acceptable Use Policy, a user is defined as any student, client, contractor, third party or visitor to SIBT, who in any way accesses SIBT IT systems or infrastructure

IT – may refer to Information Technology or to the group which provides support for Information Technology users

## 6. Related Documents

Discrimination, Harassment, Victimisation and Bullying Policy  
 Equal Opportunity and Diversity Policy  
 Privacy Policy  
 Copyright Policy

### AMENDMENT HISTORY

Department:	Academic	
Approval Authority:	Interim Academic Board	
Approval Date:	6 September 2016	
Date for Next Review:	6 September 2019	
Revision Date	Version	Summary of changes
06/09/2016	1	New Policy



## Appendix 1: Student Guide: Netiquette

The communication tools in your online unit spaces in SIBT Learning enable you to discuss curriculum related topics, to deepen your understanding of the course content and to interact with other students. Communication online is really no different from speaking face-to-face; there are certain courtesies and conventions that we try to uphold. The guidelines for how to communicate using these online tools is called Netiquette (or internet etiquette).

Although initially designed for interacting in online discussions in SIBT Learning, students might find these guidelines useful for all online communication modes including instant messaging, replying and commenting to others' posts online and even emailing.

Participating in online discussions takes some getting used to. The first few times you participate you may feel nervous about sharing your ideas publicly. The more you take part, the more comfortable you become using online communication tools and the more you will benefit from your participation.

### General politeness

An online discussion, like a face-to-face discussion, is a personal exchange of information. It can however, take place over an extended period of time: one or two days, a week or a semester. This means you can either respond immediately to discussion points or take some time to respond more carefully. Ideas and impressions are written rather than spoken, so you don't have the advantage of body language to help you interpret meaning. It is therefore, important to:

- be polite and avoid bad language;
- be tolerant of people's mistakes and contributions;
- acknowledge people's contributions;
- respect other people's point of view;
- be non-judgmental and supportive;
- avoid pasting fancy signatures, animations or graphics in your messages unless necessary for your topic;
- insert a blank line between paragraphs;
- be aware of cultural differences;
- be careful with humour and sarcasm;
- re-read your message before posting;
- consider your tone, and whether you could be misinterpreted;

One way to overcome the fact that you can't 'see' the person you are talking to is to use 'Emoticons' to give a visual meaning to your written words. Only use these if you are not asked to write using formal academic language. Only use them if you feel comfortable with them and don't overuse them.

:-) Happy	;-) Winking	:-e Disappointed	:-< Mad	:-o Surprised
:-( Sad	:D Big smile	:-D Laughing	:-I Indifferent	*-) Thinking

There is a particular shorthand used commonly on the internet which involves acronyms. You can also find these in SMS texting.

<b>BTW</b> By the way	<b>OMG</b> Oh my God	<b>IMHO</b> In my humble opinion
<b>L8R</b> Later	<b>LOL</b> Laughing out loud	<b>NP</b> No problem
<b>B4</b> Before	<b>CU</b> See you (later)	<b>AFK</b> Away from keyboard
<b>ROTFL</b> Rolling on the floor laughing		

## Basic online communication guidelines

### What should I check before I post a message?

- Read all the contributions to avoid repeating something somebody else has already written;
- Proofread your message for grammar, punctuation, spelling and layout to make the meaning clear;
- Observe and get a feel for the discussion to ensure the correct level of formality is used (this is known as *lurking*);
- Check who you are replying to. If your reply is not valuable to the whole group, reply to the author only;
- Re-read your message, and review it for appropriateness.

### What are the things I should never do?

- A discussion is public so don't write anything which discriminates on the basis of race, colour, nationality, age, marital status, sex, political affiliation, religion, disability or sexual preference, or which might be considered obscene, offensive, threatening or intimidating. This includes offensive text or pictures, for example, pornography, racism, sexism, obscenities, insults, sarcasm, defamatory statements, rumours, gossip about individuals or organisations. Such comments have no place in online communication where the general approach is supportive and collaborative. In extreme cases, people who persist in offensive or disruptive behaviour may lose access to the tool and may be charged with misconduct;
- Never publicly attack another member or post an emotionally charged contribution. This is considered *flaming* and is not acceptable;
- It is inappropriate to correct someone's mistakes in your posting to the group. If it is necessary to point out a mistake, use a private email;
- Only use capital letters for specific purposes such as headings, otherwise it can seem like SHOUTING;
- No advertising is allowed;
- Don't dominate the discussion;
- Never post when angry;
- Don't forward sensitive content without the writer's permission. This protects the confidentiality of any content that was intended only for course participants;
- Don't plagiarise – make sure all quotes and sources are properly attributed;
- Don't behave in a way that is bad-mannered. Remember, if it is inappropriate or illegal in the real world IS ALSO INAPPROPRIATE OR ILLEGAL ON THE INTERNET.

### What happens if I feel I am being harassed?

Any breach of the SIBT on electronic harassment may constitute misconduct or serious misconduct. The Student Code of Conduct for electronic communication can be found at [www.sibt.nsw.edu.au/policies](http://www.sibt.nsw.edu.au/policies)

Students should report any breaches of conduct or instances of bullying, harassment or vilification by speaking with the **Student Welfare Officer**. All such queries will be treated in confidence and SIBT aims to provide support or assistance in preventing a recurrence of the behaviour.

### What happens if I'm not sure how to contribute?

In addition to this guide, your teachers will inform you about any other rules specifically relating to participating in discussions in your course.

If you are nervous or unsure of how to participate in an online discussion, please contact your teacher. Otherwise it may be possible for your teacher to misunderstand your reasons for non-participation.