Box Hill Senior Secondary College
Acceptable Usage Policy

Guidelines and Conditions for Appropriate Use of Computer Facilities

The Box Hill Senior Secondary College network is provided for staff and students to promote educational excellence by facilitating resource sharing, innovation and communication.

Staff & students are given full access to the network with an individual account. Staff & students will also have college-administered individual electronic mail and full Internet access. Any such facilities must be regarded as privileges, which may be withdrawn for misuse of the resources.

Computing facilities are provided primarily for the educational benefit of students and the professional development of staff. Any behaviour that interferes with these primary objectives will be considered an infringement of Acceptable Use.

1. General Policies

- Use of computer/internet resources for educational purposes has priority over other (recreational) uses
- Appropriate language must be in all communications including email messages, chat and web pages
- No user may deliberately or carelessly waste computer resources (eg unnecessary printing) or disadvantage other users (eg by monopolising equipment, creating excess network traffic – for example downloading non-educational resources).
- Consideration must be given to avoiding inconvenience to other computer users. e.g.
  - use headphones to listen to resources with audio
  - leave computers ready for the next user to log in
  - not leave programs running on computers when you leave
  - not leave rubbish or paper lying around computers
  - replace furniture to normal positions when you leave.

Summary of conditions

Students & staff must not:

- Use abusive, offensive or obscene language or images in any communications
- Steal, or deliberately or carelessly cause damage to any equipment
- Interfere with or change any software settings or other people’s files
- Attempt to get around or reduce network security
- Do anything in any other person's home directory
- Store unauthorised types of files in their own home directories
- Send "spam" (bulk and/or unsolicited e-mail)
- Reveal personal information about members of the school community in any communications
- Deliberately enter, or remain in, web sites containing objectionable material
- Knowingly infringe copyright and privacy laws
- Users are encouraged to regularly maintain their individual hard drive to optimise performance (e.g. transfer older files to CD or disk, run virus software, remove unwanted files)
2. Computer hardware

Computer facilities are expensive, sensitive and must be treated carefully. Students & staff must not:
- Do anything likely to cause damage to any equipment, whether deliberately or carelessly
- Steal equipment
- Vandalise equipment
- Mark or deface any equipment
- Interfere with networking equipment such as hubs
- Eat or drink near any College owned computer resources
- Use CD ROM drives for non-educational purposes (e.g. playing audio CD’s, copying files other than their own work files)

Students & staff must not, without permission:
- Attempt to repair equipment
- Unplug cables or equipment (e.g. swapping keyboards, mouse, network and power cables)
- Move equipment to another place
- Remove any covers or panels
- Disassemble any equipment
- Disable the operation of any equipment

Students & staff must report damage and other faulty equipment. Students should report other people breaking these rules.

Regardless of the real or supposed levels of understanding, students & staff are NOT authorised to attempt the repair or adjustment of any college hardware or software. Any such attempt will be regarded as a violation of network security. Any problem with equipment or software must be referred to an authorised person.

3. Software and operating systems

Computer operating systems and other software must be set up properly for computers to be useful.

Students & staff will not:
- Change any computer settings (including screen savers, wallpapers, desktops, menus standard document settings etc) without permission
- Bring or download unauthorised programs, including games, to the college or run them on college computers. Online internet games are not permitted on the College network.
- Delete, add or alter any configuration files
- Copy any copyrighted software to or from any computer, or duplicate such software
- Deliberately introduce any virus or program that reduces system security or effectiveness

4. Networks

Network accounts are to be used only by the authorised owner of the account. Any files stored on the College network are for educational purposes only. It is not to be used to store private files of individuals.

If you find a computer logged in, you should do nothing in that account except log out.
It is the responsibility of students & staff to make backup copies of their work. The college will exercise due care with backups but will not be held responsible for lost data.

Students & staff must not:
- Attempt to log into the network with any user name or password that is not their own, or change any other person’s password
- Reveal their password to anyone except the system administrator or classroom teachers, if necessary. Students & staff are responsible for everything done using their accounts, and everything in their home directories. Since passwords must be kept secret, no user may claim that another person entered their home directory and did anything to cause college rules to be broken.
- Use or possess any program designed to reduce network security
- Enter any other person’s home directory (drive H:) or do anything whatsoever to any other person’s files
- Attempt to alter any person’s access rights
- Store the following types of files in their home directory, without permission from the Computer Systems Manager:
  - Program files (EXE, COM)
  - Compressed files (ZIP, ARJ, LHZ, ARJ, TAR etc)
  - Picture files, unless they are required by a subject
  - Obscene material – pictures or text
  - Obscene filenames
  - Insulting material
  - Password-protected files
  - Copyrighted material
- Intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.

5. Printing

Students & staff must minimise printing at all times by print previewing, editing on screen rather than on printouts and spell-checking before printing.

Students must not load paper into printers without permission. Paper that is pre-used, torn, creased, damp, irregularly shaped or sized or unsuitable for laser printers should not be used in laser printers.

NB Students must ensure that a positive print credit balance is maintained that will meet the class and teachers requirements.

6. Internet usage

Internet access has been provided to assist students’ learning. Students must use it only with permission in timetabled classes, as instructed by the classroom teacher. Outside of timetabled classes (e.g. library), students are to follow the College’s general computer usage policy.

Because the Internet is an unsupervised environment, the school has a responsibility to ensure that, as far as possible, material obtained from the Internet is not offensive or inappropriate. To this end, filtering software has been placed on the Internet links. In the end, however, it is the responsibility of individual students to ensure their behaviour does not contravene college rules or rules imposed by parents/guardians.
The school is aware that definitions of "offensive" and "inappropriate" will vary considerably between cultures and individuals. The school is also aware that no security system is perfect and that there is always the possibility of inappropriate material, intentionally and unintentionally, being obtained and displayed.

It is the responsibility of the school to:
- provide training on the use of the Internet and make that training available to everyone
- make users aware of the School Internet Access Policy
- take action to block the further display of offensive or inappropriate material that has appeared on the Internet links

6.1 Email:
Electronic mail is a valuable tool for personal and official communication both within the college network and on the Internet. Students and staff are encouraged to use it and take advantage of its special features. As with all privileges its use involves responsibilities.

Since students & staff are given free email accounts by the College, no other email accounts may be used at the College. If you have other email accounts, you must check for mail and collect it at home. Other email accounts, such as Hotmail, must not be used on the College computers.

Throughout the Internet there are accepted practices known as Netiquette which should be followed. The following points should be noted:

- Use appropriate language and be polite in your messages. Do not be insulting, abusive, swear or use vulgarities.
- Never write hate mail, chain letters, harassment, discriminatory remarks and other antisocial behaviours. Therefore no messages should contain obscene comments, threats, sexually explicit material or expressions of bigotry or hate.
- Do not reveal your personal address or the phone numbers of students or colleagues.
- Note that email is not guaranteed to be private. System administrators do have access to all files including mail. Messages relating to illegal activities may be reported to the authorities.
- Teachers will set their own guidelines for use of electronic mail in class time to support teaching and learning. e.g. email of work to students and electronic submission of work

Students & staff will not:
- send offensive mail
- send unsolicited mail to multiple recipients ("spam")
- send very large attachments
- use email for any illegal, immoral or unethical purpose
- attempt to disguise their identity or the true origin of their mail
- forge header messages or attempt to use any mail server for deceptive purposes
- use any mail program designed to send anonymous mail

6.2 Chat lines (IRC, MIRC, ICQ etc)
Real-time chat programs (MIRC, ICQ) are not to be used by students unless instructed by a teacher.
6.3 World Wide Web

The World Wide Web is a vast source of material of all sorts of quality and content. The college will exercise all care in protecting students from offensive material, but the final responsibility must lie with students in not actively seeking out such material.

It is conceivable that, especially for senior students, information is required for curriculum purposes that may appear to contravene the following conditions. In such cases, it is the responsibility of students and teachers to negotiate the need to access such sites.

- Students & staff will not deliberately enter or remain in any site that has any of the following content:
  - Nudity, obscene language or sexual discussion intended to provoke a sexual response
  - Violence
  - Information on, or encouragement to commit any crime
  - Racism
  - Information on making or using weapons, boobytraps, dangerous practical jokes or "revenge" methods
  - Any other material that the student's parents or guardians have forbidden them to see

- If students encounter any such site, they must immediately turn off the computer monitor (not the computer itself) and notify a teacher. Do not show your friends the site first.

- The Internet must not be used for commercial purposes or for profit.

- The Internet must not be used for illegal purposes such as spreading computer viruses or distributing/receiving software that is not in the public domain.

- It is inappropriate to act as though you intend to break the law e.g. by attempting to guess a password or trying to gain unauthorised access to remote computers. Even if such attempts are not seriously intended to succeed, they will be considered serious offences.

- Interactive use of the Internet should ensure that there is no possibility of the transmission of viruses or programs which are harmful to another user's data or equipment.

- Copyright is a complex issue that is not fully resolved as far as the Internet is concerned. It is customary to acknowledge sources of any material quoted directly and it is a breach of copyright to transmit another user's document without their prior knowledge and permission. This includes the use of images and text. It is safest to assume all content on web sites is the legal property of the creator of the page unless otherwise noted by the creator.

- Privacy – for further information please refer to the Privacy document

6.4 The College Web site

Material placed onto the school web site must:

- be checked for appropriateness and (as far as possible) accuracy

- not violate copyright

- have the written permission of a parent/guardian if the parent or guardian has requested such a veto

- not contain the full name accompanied by an image, the home address or home phone number of an individual

- not contain the e-mail or web address of a student unless specifically required and requested

Links to sites beyond the school site must be checked for appropriate content. It must be recognised that the content of external sites may change after links have been made, and the
college cannot be held responsible for the contents of linked sites, but the college must exercise all due care to ensure no objectionable material is directly accessible via links on our site.
7. Possible penalties
More than one may apply for a given offence. Serious or repeated offences will result in stronger penalties.

- Temporary ban on using computers
- Removal of email privileges
- Removal of internet access privileges
- Removal of network access
- Paying to replace damaged equipment
- Removal from classes where computer use is involved
- Suspension from College

Criminal charges may be laid with the police.

8. Staff Information

8.1 Staff responsibilities
College expectation on staff responsibilities regarding student access to ICT resources (see attached process – Appendix 1)

Supervision of students in POD’s or other areas where there is not direct supervision

8.2 Internet access and email
As an employer provides these resources, there is an underlying implication that they are to be used for work purposes.

Emails sent through a work email are not private communications. The College administration and DET have authority to view emails

Emails regarding College incidents must be preserved for seven (7) years, as they are ‘discoverable’ documents in legal proceedings.

8.3 Privacy and copyright
Whilst privacy legislation does not prevent the use of student images and/or names on websites, it is DET policy not to do so.

Students own the copyright to the work that they produce. However, schools own the work that is produced by staff as part of their job (Intellectual Property)

8.4 Data Handling
The Privacy Act requires schools to ensure all personal data is properly stored. This is done by:

- Ensuring restricted access to the appropriate people
- Laptop hard drives are not a secure location and care must be taken to secure sensitive information about individuals