Auburn
High School

Burgess Street East Hawthorn Victoria 3123
Provider: DEECD CRICOS Code: 00861K
Telephone 9822 3247 Fax 9822 6837 Principal MARTIN CULKIN
eMail hawthornsc@edumail.vic.gov.au
Website www.auburnhs.vic.edu.au

ACCEPTABLE ICT and INTERNET USE POLICY

1. Policy Statement

The internet offers huge potential benefits for teaching and learning. It offers wonderful opportunities for students and teachers to contribute to the world community on the web. Blogs, social networking spaces such as Face book and instant messaging tools such as MS Messenger are now part of students' 'life on the web'. Students can:

- explore the world online
- visit museums and libraries around the world
- access rich information resources to support research and investigations
- communicate and collaborate with people all over the world
- publish to the web.

Auburn High School has an important role in preparing students for these 'online communities', even though students may not access some online communities at school (eg Facebook).

Before using the school's Internet, it's crucial to make sure all users, staff, students and visitors understand what they should and shouldn't be doing online.

Behaving safely online means:

- protecting their own privacy and personal information
- selecting appropriate spaces to work and contribute
- protecting the privacy of others (this can be sharing personal information or images)
- being proactive in letting someone know if there is something is 'not quite right'. At home this would be a parent or guardian, at school a teacher.

These principles of safety and responsibility are not specific for the web but certainly apply to the use of internet at school. Just as in the real world, the virtual world of the internet involves some risks. Auburn High School has developed proactive strategies that help to minimise these risks to our students.

2. Guidelines

- Use of the school's network to access the Internet and Internet services, including electronic mail and the World Wide Web, will governed by an Acceptable Use Procedures (AUP) for the Internet.
- The Acceptable Use Procedures (AUP) is intended to encourage responsible action and to reflect a respect for the ability of its adherents to exercise good judgement.
- Independent student use of the internet will only be permitted where students and their parents/carers provide written acknowledgement that students agree to act in accordance with the standards of conduct established in the Acceptable Use Procedures (see appendix-a).
- Students can expect sanctions if they act irresponsibly and disregard their obligations to other users and the school as the provider of their Internet access. Staff are required to become familiar with the Department's acceptable use policy Acceptable Use Policy for

DEECD Information, Communications and Technology (ICT) Systems - Departmental Policies - About the Department of Education and Early Childhood Development

- Students must not use the school internet, computers and digital learning devices or the ICT network in breach of a law or to commit an offence. This includes cyber-bullying and sexting, and breaches of copyright.

3. Program

- The use of the school's digital learning network is subject to the Acceptable Use Procedures (see appendix-a). Briefly this means that the school's network can be used only by staff, students and associated individuals (eg visiting teachers) and only for or in connection with the educational or administrative functions of the school.
- The Acceptable Use Procedures (AUP) is intended to operate within and be consistent with existing school policies and procedures in areas such as:

Anti-bullying (including cyber-bullying) and Anti-harassment Student Welfare & Engagement Policy

- Responsibility and accountability for network security is the shared responsibility of all network users. It is the responsibility of the student to protect his/her password and not divulge it to another person. If a student knows or suspects his/her account has been used by another person, the account holder must notify a teacher immediately.
- All messages created, sent or retrieved on the school's network are the property of the school, and should be considered public information. The school reserves the right to access and monitor all messages and files on the computer system as deemed necessary and appropriate. Internet messages are public communication and are not private. All communications including text and images can be disclosed to law enforcement and other third parties without prior consent from the sender.
- Independent student use of the internet on the school's network will only be permitted where students and their parents/carers provide written acknowledgement that students agree to act in accordance with the standards of conduct established in this policy document and as set-out in the Acceptable Use Procedures (AUP)
- For breaches of the Acceptable Use Procedures students can face a number of consequences depending on the severity of the breach and the context of the situation. More than one consequence may apply for a given offence. Serious or repeated offences will result in stronger penalties.

  Removal of network access privileges

  Removal of email privileges

  Removal of internet access privileges

  Removal of printing privileges

  Paying to replace damaged equipment

  Other consequences as outlined in the school's Student Welfare & Engagement policy.

- Bullying and harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual or group's race' religion, national origin, physical attributes, or sexual preference will be transmitted. Violations of any guidelines listed above may result in disciplinary action.
- While the Internet may be largely a self-regulated environment, the general principles of law and community standards still apply to communication and publishing via the Internet. In addition to school penalties, there are legal sanctions for improper use of the Internet.

4. LINKS AND APPENDICES (including processes related to this policy).

Links which are connected with this policy are:

- The school's Anti-bullying (including cyber-bullying) and Anti-harassment Policy
- The school's Student Welfare Engagement Policy
- Acceptable Use Procedures (AUP) for the Internet
- http://www.education.vic.gov.au/management/elearningsupportservices/www/classroom/default.htm
- http://www.education.vic.gov.au/management/elearningsupportservices/www/classroom/technologies.htm
- http://www.education.vic.gov.au/management/elearningsupportservices/www/management.htm
- Appendix A contained herein.

5. EVALUATION

This policy will be reviewed annually or more often if necessary due to changes in regulations or circumstances.

Appendix-A Guidelines and Conditions Acceptable Use Procedures for the School's Internet

The school's 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 is for **educational purposes only**
- Access to the Internet will be supervised by a staff member
- Appropriate language must be used in **all** communications
- Internet and printing services are both charged against a student's account.
- Consideration must be given to avoiding inconvenience to other computer users. e.g. use headphones to listen to sound or music; leave computers ready for the next user to log in; do not leave programs running on computers when you leave; do not leave rubbish or paper lying around computers; replace furniture to normal positions when you leave

Summary of conditions

Students must not:

- Use abusive or obscene language in any communications
- Steal, or deliberately or carelessly cause damage to any equipment
- Interfere with or change any software settings or other user's files
- Attempt to get around or reduce network security
- Logon using another user's account
- Store unauthorised types of files in their own home directories (games or other executables)
- Send "spam" (bulk and/or unsolicited e-mail)
- Reveal personal information in any communications
- Deliberately enter, or remain in, web sites containing objectionable material
- Knowingly infringe copyright

2. Computer hardware

Computer facilities are expensive and must be treated carefully.

Students must not:

- Do anything likely to cause damage to any equipment, whether deliberately or carelessly
- Interfere with networking equipment
- Eat or drink near any School owned computer resources

Students must not, without permission:

- Attempt to repair equipment without permission
- Unplug cables or equipment
- Move equipment to another place
- Remove any covers or panels
- Disassemble any equipment
- Disable the operation of any equipment

  Students must also report other people breaking these rules.

Regardless of the real or supposed levels of understanding, students 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 reported to a teacher or technician.

3. Software and operating systems

Computer operating systems and other software are set up properly for computers to be successfully used in the School.

Students will not:

- Change any computer settings (including screen savers, wallpapers, desktops, menus standard document settings etc)
- Bring or download unauthorised programs, including games, to the college or run them on college computers, online Internet games are banned
- 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.

It is the responsibility of students to ensure their user account details remain secure and that unauthorised use of their account does not take place.

Students must not:

- Attempt to log into the network with any user name or password that is not their own
- **Reveal their password to anyone. Students 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 F:) or do anything whatsoever to any other person's files
- Be logged on to the network on different computers at the same time
- Store the following types of files in their home directory:
    - Program files (EXE, COM)
    - Compressed files (ZIP, ARJ, LHZ, ARJ, TAR etc)
    - Picture files, video files, music files etc unless they are required for a school task
    - Obscene material – pictures or text
    - Obscene filenames
    - Insulting material
    - Copyrighted material
- Intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.

5. Printing

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

6. Internet usage

Internet access is expensive and has been provided to assist students' education. Students must use it only with permission, and not in any unauthorised way. Students are to be supervised by a staff member when using the Internet at all times.

The Internet is not intended for entertainment.

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/carers.

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.

6.2 Email

Note: At this stage we do not permit students at Insert school name here to have school email accounts. In the event of this occurring, the following guidelines apply.

Electronic mail is a valuable tool for personal and official communication both within the school 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.

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. **All school emails are filtered for inappropriate content.** Messages containing inappropriate content are automatically reported to the ICT Manager.
- Teachers will set their own guidelines for use of email in class time.
  Students will not:
- Send offensive mail
- Send unsolicited mail to multiple recipients ("spam")
- Use email for any illegal, immoral or unethical purpose

6.3 Chat lines (IRC, MIRC, ICQ etc)

Real-time chat programs (MIRC, ICQ etc) are **not** to be used by students.

6.4 World Wide Web

The World Wide Web is a vast source of material of all sorts of quality and content. The school 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 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, booby traps, 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.

6.5 The School 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 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 school cannot be held responsible for the contents of linked sites, but the school must exercise all due care to ensure no objectionable material is directly accessible via links on our site.

7. Penalties

More than one may apply for a given offence. Serious or repeated offences will result in stronger penalties.

- **Removal of network access privileges**
- **Removal of email privileges**
- **Removal of internet access privileges**
- **Removal of printing privileges**
- **Paying to replace damaged equipment**
- **Other consequences as outlined in the school discipline policy**
- **Removal of the computer or iPAD from student**

8. The Parent Information Kit is to be read and the Agreement Form is to be signed and returned to school before access to the school's Information and Technology resources can be granted**.**

Return Sheet Auburn High School

Part A– Agreement to be signed by the student and parent.

See part C for support information.

When I use technology, both at school and at home I have responsibilities and rules to follow. I agree to:

- be a safe user whenever and wherever I use that technology
- be responsible whenever and wherever I use technology and support others by being respectful in how I talk to and work with them and never write or participate in online bullying (this includes forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviour)
- report to an adult if I feel unsafe or uncomfortable online or see a friend being unsafe or being made to feel uncomfortable by others.

When at school I agree to:

- behave according to the school Code of Conduct when online or using mobile technology
- keep myself and my friends safe by not giving out personal details including full names, telephone numbers, addresses and images and protecting my password
- use the technology at school for learning, use the equipment properly and not interfere with the work or data of another student
- not bring or download unauthorised programs or files
- not go looking for rude or offensive sites
- use an 'online name' and avatar when sharing my work online
- remember that the content on the web is someone's property and ask my teacher or parent to help me get permission if I want to use information or pictures
- think carefully about what I read on the internet, question if it is from a reliable source and use the information to help me answer any questions (I should not copy and paste the information as my answer)
- talk to my teacher or another adult if:
    - I need help online
    - I am not sure what I should be doing on the internet
    - I come across sites which are not suitable
    - someone writes something I don't like, or makes me and my friends feel uncomfortable or asks me to provide information that I know is private
- I feel that the welfare of other students at the school are being threatened.

This Acceptable Use Policy also applies to students during school excursions, camps and extra-curricula activities

I acknowledge and agree to follow these rules. I understand that my access to the Internet and mobile technology at school will be renegotiated if I do not act responsibly.

Student Name

_____

Student Signature

_____

Parent Permission

I agree to allow my child to use the internet at school. I have discussed the scenarios, potential problems and responsible use of the internet with him/her as outlined in the internet use kit.
I will contact the school if there is anything here that I do not understand. If there is a situation which concerns me, I will contact either the school or ACMA Australia's Internet safety advisory body on 1800 880 176.

Parent/Guardian Signature _____

Date _____

When this Acceptable Use Agreement for the use of the school's internet has been completed and signed please return it to the School.

On receipt of the completed and signed Acceptable Use Agreement you will receive your network and internet account details.

Please detach this return slip from the *Guidelines and Conditions Acceptable Use Procedures for the school's Internet* document before it is returned to the campus.