INTERNET USERS 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 Facebook 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

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

Before our students start to explore the Internet, it's crucial to make sure everyone understands what they should and shouldn't be doing online.

Behaving safely online means:

- protecting their own privacy and personal information (we used to call it 'stranger danger')
- 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 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.

Oberon High School has developed proactive strategies that help to minimise these risks to our students.
2. **GUIDELINES**

2.1 Use of the school’s network to access the Internet and Internet services, including electronic mail and the World Wide Web, will be governed by an Acceptable Use Procedures (AUP) for the Internet.

2.2 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.

2.3 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).

3. **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 Facebook 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

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

Before our students start to explore the Internet, it's crucial to make sure everyone understands what they should and shouldn't be doing online.

Behaving safely online means:

- protecting their own privacy and personal information (we used to call it 'stranger danger')
- 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 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.

Oberon High School has developed proactive strategies that help to minimise these risks to our students.

4. **GUIDELINES**

4.1 Use of the school’s network to access the Internet and Internet services, including electronic mail and the World Wide Web, will be governed by an Acceptable Use Procedures (AUP) for the Internet.

4.2 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.

4.3 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).

4.4 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.

4.5 Students must not use the school network in breach of a law or to commit an offence.

5. **PROGRAM**

5.1.1 The use of the school's 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 (e.g. visiting teachers) and only for or in connection with the educational or administrative functions of the school.

5.1.2 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

5.2.1 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.

5.2.2 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.

5.3.1 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).

5.3.2 For breeches 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, such as:

- 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 discipline policy

5.4 Bullying and harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual or groups race, religion, national origin, physical attributes, or sexual preference will be transmitted. Violations of any guidelines listed above may result in disciplinary action.

5.5 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.

6. 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 Policy

Appendices which are connected with this policy are:
- Appendix A: Acceptable Use Procedures (AUP) for the Internet
- Appendix B: Return Slip – Acceptable Use Agreement for the use of school’s internet

7. EVALUATION

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

Acceptable Use Procedures (AUP) for the 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 must 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)

1.1 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 referred to an authorised person.

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 C 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.

Students are allocated printing credit as part of their ICT Parent Payment. Once this allocation has been completely used, further allocations may be purchased. Students are not to use another student’s allocation. Students who deliberately waste another student’s allocation will be liable for all costs incurred. Students are charged a fee to printed A4 page of black 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.

Students are allocated a download credit as part of their ICT Parent Payments. Once this allocation has been completely used, further allocations may be purchased. Students are currently charged for each Mb of download.

6.1 **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 school 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**

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 college 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 (www)

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 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.

**Students must understand:**
• 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:
  o 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
  o 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’s Website

*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 college 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 consequence may apply for a given offence. Serious or repeated offences will result in stronger penalties, such as:
• 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 discipline policy
Appendix B

**Return Slip – Acceptable Use Agreement for the use of school’s Internet**

Before you may use computer facilities at the school, you must sign this contract, which binds you to the following conditions. If you break any of the conditions, appropriate penalties will be applied.

**Student’s Name:** ___________________________  **Form:** ___________________________

I have read the Guidelines and Conditions for Acceptable Use Procedures for the School’s Internet document and agree to obey the guidelines and conditions in it.

**Student’s Signature:** ___________________________  **Date:** ___________________________

**Parent/Guardian Permission**

*The parent or legal guardian of the student must complete this section.*

I, the parent or guardian of ___________________________ have read and understand the Guidelines and Conditions for Acceptable Use Procedures for the School’s Internet. I agree that my child shall observe these guidelines and conditions.

**Parent/Guardian’s Name:** ___________________________

**Parent/Guardian’s 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 school.