Acceptable Network Usage Policy

Purpose:

The Lumen Christi Catholic College computer network is provided for staff and students to facilitate resource sharing, innovation and communication. All students are given access to the computer network through College computers with an individual account. Students will also have College administered individual email and filtered 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Any such facilities must be regarded as privileges which may be withdrawn for misuse of the resources.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.

Any and all internet enabled devices and internet communications may be monitored or inspected by the Principal and/or delegate if it is deemed necessary to ensure that policies are being followed.

Policy:

1. General Policies

- Use of computer/internet resources for educational purposes has priority over other (recreational) uses.
- Appropriate language must be used 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, network traffic etc).
- 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; 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.
- Do not use another person’s log on details.
- Bluetooth communication between computers and other Bluetooth enabled devices is not allowed at the College.
Summary of conditions

Students must not:

- Use abusive or obscene language in any communications.
- Take without permission, 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 or shared directories.
- Waste resources.
- Send “spam” (bulk and/or unsolicited e-mail).
- Reveal personal information in any communications.
- Deliberately enter, or remain in, web sites containing objectionable material or knowingly infringe copyright.

1. Computer hardware

Computer facilities are expensive, sensitive and must be treated carefully.

Students must not:

- Do anything likely to cause damage to any equipment, whether deliberately or carelessly, including stealing equipment or vandalising equipment (e.g. graffiti).
- Interfere with networking equipment such as hubs, switches, wireless access points or network connections.
- Eat or drink near any College owned computer resources.
- Attempt to repair equipment.
- Unplug cables or equipment.
- Move equipment to another place (with the exception of student issued laptops).
- Remove any covers or panels.
- Disassemble any equipment.
- Disable the operation of any equipment.

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.

Students must also report other people breaking these rules.

2. Software and operating systems

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

Students 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.
• 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.

3. Networks

Network accounts are to be used only by the authorised owner of the account. If you find a computer logged in, you should do nothing in that account except log out.

It is the responsibility of students to make backup copies of their work. The College will exercise due care with backups of College network home drives but will not be held responsible for lost data. (See Technical Support and Data Back-up Guidelines).

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.

Students 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.
• Enter any other person’s home directory 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 or shared network drives, without permission from the Principal and/or delegate:
  • Program files (EXE, COM).
  • Compressed files (ZIP, ARJ, LHZ, ARJ, TAR etc).
  • Batch files (BAT, CMD).
  • 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.

4. Printing

• Students must minimise printing at all times by print previewing, editing on screen rather than on printouts and spell-checking before printing. Teacher permission must be obtained before a student may print out any material.
- 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.

5. 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. It 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 built into the College internet structure. In the end, however, it is the responsibility of individual students to ensure their behaviour does not contravene College rules. The College 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. Students must not intentionally attempt to search for and browse web content that is inappropriate. Students must not attempt to by-pass filtering systems, including the use of Proxy Bypassing software or websites.

6. Email, Blogging, Messaging, Forums

- E-mail is a valuable tool for personal and official communication both within the College network and on the internet. Students are encouraged to use it and take advantage of its features, as with all privileges its use involves responsibilities.
- Students are given free email accounts by the College, other email accounts such as Hotmail must not be used on 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 use insulting or abusive language, swear or use vulgarities.
  - Never write hate mail, chain letters, harassment, discriminatory remarks and other antisocial behaviours.
  - No messages should contain obscene comments, threats, sexually explicit material or expressions of bigotry or hate.
  - No message should contain false or defamatory information about a person or organisation.
  - Do not reveal your personal address or the phone numbers, other student personal information or staff personal information to others.
  - Note that email is not guaranteed to be private. System administrators do have access to all files including mail.
  - Messages and/or images sent and received, relating to illegal or inappropriate activities may be reported to the authorities.
- Appendix ii Acceptable Network Usage Policy v2.3 8th December 2010
- Teachers will set their own guidelines for use of electronic mail in class time. A possible practice is for students to be given a small amount of time at the beginning and/or end of a lesson in which they may check their mail but the use of electronic mail during class time is at the discretion of the teacher.

Students 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.

7. Chat lines (IRC, MIRC, ICQ etc)

- Real-time chat programs (MIRC, ICQ, MSN) are not to be used by students unless instructed by a teacher.

8. 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 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.
  - Information on making or using weapons, booby traps, dangerous practical jokes or "revenge" methods.
  - Any other material that the College or 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 (including on-line auction sites eg e-Bay) or for profit.
  - Illegal purposes such as spreading computer viruses or distributing/receiving software that is not in the public domain.
  - Acting 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 must be considered at all times. Students will observe appropriate copyright clearance, including acknowledging the author or source of any information used. Students must never plagiarise. All students must acknowledge sources of any material quoted directly and it is a breach of copyright to transmit another person’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. Appendix ii Acceptable Network Usage Policy v2.3 8th December 2010

9. The College Web site and other Web based repositories

- Material placed on the World Wide Web must:
  - Be checked for appropriateness and (as far as possible) accuracy.
  - Not violate copyright.
  - Have the written permission of a parent/guardian if required.
  - 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 College 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.

10. Possible penalties

- Any breach of the Acceptable Usage Policy may result in:
  - Ban on lunchtime computer use.
  - Temporary ban on using computers.
  - Removal of email privileges.
  - Removal of internet access privileges.
  - Removal of home directory and network.
  - Detention, suspension or exclusion from the College.
  - Paying to replace damaged equipment.
  - Removal from classes where computer use is involved.
  - Referral to appropriate agencies.
  - Removal of home use of laptops from Laptop Program.
  - Confiscation of laptops from Laptop Program.

References:

LCCC Computer Use Agreement
LCCC IT Policy
LCCC ICT Policy

Forms:

Approved by: Paul Carroll
Revision Date: October 2012
Next Revision Date: October 2014
Implementation Date: October 2010
Issuing Group: Lumen Christi Catholic College Executive
Contact Officer: Derek Gillions