St Francis Xavier’s Regional Catholic School

Communication/Network Use Policy

General Principles

- As part of the curriculum, students are permitted access to the computer network and certain on-line facilities such as the Internet and Email.
- Access to the computer network is a privilege which may be enjoyed as long as certain standards are observed. These standards are set out in this Policy. If these standards are not observed, privilege of access may be withdrawn. The consequences for breaching these standards are set out in Section 5 (Consequences for Mis-Use of the Computer Network) of this Policy.
- Students must understand that their access to the computer network is only allowed for acceptable and ethical purposes. By “acceptable”, we mean that use must only be along the lines of the acceptable uses set out in Section 2 (Acceptable Uses) of this Policy. By “ethical”, we mean that students are not allowed to breach standards of common decency, or manners, and must not break any laws. This is explained in more detail within Section 4 (Ethical Uses) of this Policy.
- Students are expected to be responsible and ethical in their use of the computer network, at all times.

STUDENTS’ RESPONSIBILITIES

Section 1 - Access to the Computer Network
Subject to complying with this Policy, all students have the right to equal access to network resources.

No student should monopolise a computer or the network used by it. Students should not play games or use the computer network for non-academic purposes. This applies at all times.

Section 2 - Acceptable Uses
The following uses of the computer network are considered acceptable:

- to use in connection with curriculum activities
- to research projects or assignments
- to send and receive email (academic purposes only)
- to explore the Internet in connection with curriculum activities and along guidelines set out by the staff.
- to use programs supplied and authorised by the school
- to use only equipment provided by the school (floppy disks and USB drives being the only exceptions)

A student’s use of the computer network for purposes other than those above may be considered to be unacceptable. Some of the uses considered unacceptable by the school are outlined in Section 3 – Unacceptable Uses. Please note that unacceptable uses are not limited to this list. The list is provided to act as a general guide. Other areas of unacceptable use may be added or acted upon at the school’s discretion. Where the school determines that a student’s use of the computer network is unacceptable, the consequences in Section 5 of this Policy will apply.

Section 3 - Unacceptable Uses
The following uses of the computer network are considered unacceptable:

- using the connection with non-curriculum activities (this includes games especially)
- to upload or download non-academic related files / software
- to bring into the school or distribute or copy software
- to install software not authorised by the school
- to install software that is not licensed by the school
- to copy software or music illegally
- to send and receive non-academic email
- to explore the Internet in connection with non-curriculum
- to use the network for commercial use
- to use the network to hack into user information or computers within the school
- to use the network to hack into computer networks and information within entities external to the school (ie other schools, government agencies, etc).
• to use programs not supplied and authorised by the school
• deliberately introducing computer viruses, malicious code (including trojans, worms, viruses, time bombs, etc)
• forging documents or copying another person’s work without permission
• neglecting to check floppy disks or other removable media for computer viruses
• to use storage both on individual computers and the network without permission or gain access to storage areas not authorised by ICT (especially for the purpose of storing non-academic materials or to gain access to unauthorised information)
• to use methods in an attempt to hide or mislead to the location of unacceptable and unauthorised files and software (within personal storage or another person's storage area)
• to use equipment not provided by the school (floppy disks and USB drives being the only exceptions)

Where the school determines that a student’s use of the computer network is unacceptable, the consequences in Section 5 of this Policy will apply.

Section 4 - Ethical Issues
Students must be ethical in using the computer network.

What constitutes ethical behaviour is an evolving concept. Listed below are some examples of behaviour, which are considered not to be ethical in the use of the computer network. This list is not final, and is provided by way of example only.

In its sole discretion, the school may determine that other forms of behaviour not listed below are also unethical.

Where the school determines that a student’s use of the computer network is unethical, the penalties in Section 5 of this Policy will apply.

For example, when using the computer network, students must not:

• deliberately attempt to damage the equipment (this can be by fiddling with equipment)
• Be impolite, abusive or indecent toward anybody else
• Harass or be discriminatory toward anybody else (either sexually, racially or in any other way)
• Violate general standards of common sense, decency or etiquette
• Do anything illegal
• Disclose the personal details of any other student, staff member or other person
• Access any Internet sites or subject matter which have been specifically banned by the school
• Access or attempt to access inappropriate material on the Internet
• Breach another person's copyright in any material
• Interfere in any way with the legitimate work of other computer network users
• Upload or download any software (without approval by ICT staff)
• Use the computer network for commercial or profit-making exercises
• Purchase goods or services via the computer network
• Use the computer network to gain unauthorised access to any other computer network (i.e. hacking)
• Spread computer viruses
• Use any other person’s password to access the computer network
• Impersonate anybody else or use pseudonyms, or forge email messages
• Disclose their passwords or accounts to anyone
• Use inappropriate language in documents and email correspondence
• Use disks without permissions of a class teacher or authorised staff member.

When using the computer network, students MUST at all times:

• Respect the equipment
• Be polite and courteous
• Use appropriate language
• Notify a teacher or ICT Staff if they have breached this Policy, or if they become aware that any other student has done so
• Comply with standards of public decency
• Respect the rights of other computer users
• Observe that copyright exists in other people’s work on the computer network
• Obey the law
• Comply with this Policy.
Section 5 - Consequences for Mis-use of the Computer Network and Equipment

In accordance with the Behaviour Management Policy, students who break the rules in using ICT equipment and facilities will go on a step. Students reaching step 4 within a week will go to the planning room for one hour. More serious offences result in students being fast tracked to step 4.

Alternately teachers can recommend immediate action for repeated and / or more serious offences which may result in:

- Students losing the privilege of using the ICT equipment and facilities for a period of time
- Students being billed for damages caused through misuse of the equipment and facilities
- Students being suspended
- The school cooperating with the police and other authorities in any investigation relating to the illegal uses of the computer network.

Section 6 - Network Privacy and Security Issues

Students should be aware that their electronic communication and work created via the schools computer network is not private, and that staff may access their work. This extends to:

- Files in connection with their curriculum
- Incoming and outgoing email communications
- Sites accessed on the Internet.

The school reserves the right to screen students' files and work to ensure that the computer network is being used for acceptable purposes and in accordance with this Policy.

In addition, the students' files may be accessed by the school's ICT Staff as part of normal maintenance procedures. “Normal maintenance” includes spot checks to ensure that inappropriate materials, or works subject to another persons copyright, are not being kept in private folders and inappropriate Internet sites have not been visited.

Further to this students must:

- Inform staff of breaches to privacy and security as soon as practical
- Be responsible for their own passwords and security
- Not leave computers logged on or allow others to use their logon
- Not lock the computers so no-one else can use them
- Install any software designed to compromise the network, other users’ privacy or security.
- Not attempt to bypass network security by using any software or devices

Failure to comply with Network Security and Privacy issues will result in the penalties listed in Section 5 being applied.

Section 7 - Equipment Care

Students should be respectful of equipment and not intentionally misuse equipment to the extent that it becomes damaged, as this affects all users that wish to the equipment. In particular students must:

- Respect the equipment
- Report any faults, difficulties or breaches in a timely manner to staff or ICT
- Report damage as soon as possible

Section 8 - Storage of Files

Students are expected to be mindful of the space they are using on the network and are responsible for ensuring they:

- Store only school related work
- Manage their own files (this includes deleting files when no longer needed or organising for them to be backed up to take home)
- Manage their email by regularly reading emails and removing unwanted emails
- Follow instructions by teachers and ICT Staff for the maintenance of their own personal space

Section 9 - Safety

Students should not do anything to the computer network which may possibly jeopardise their personal safety either at school or outside school.
In particular, students must not:

- give out any identifying details such as their home address or telephone number, or school name in a public chat or bulletin board. Students should only disclose those details personally known to them
- give out personal information such as age, marital status or financial position of anyone
- arrange a meeting in person with another person they have “met” or only communicated with by computer, without prior parental approval. If a meeting is arranged, it should be in a public place in the presence of a parent or responsible adult
- respond to messages or bulletin board items that are indecent, suggestive, belligerent, discriminatory, threatening, or which make the students feel uncomfortable or unsafe in any way.

In addition, students:

- must tell their teacher, the system administrator or their parents if an indecent, suggestive, discriminatory or threatening message in encountered. The school will then make a copy of that message and refer it to the appropriate authorities, including the police if necessary
- should be aware that people they “meet” or communicate with on-line may pretend to be someone else
- should remember that everything they read on line may not be accurate
- should avoid offers which involve either financial transactions or personal meetings

Section 10 - Limitation of Liability
Students will be allowed access to the computer network as part of the core curriculum activities. It is not practical that every student will be supervised individually when using the computer network, and the school expects students to act responsibly and sensibly.

The school does not accept any liability which may result from any students unacceptable or unethical uses of the computer network.

If there are any concerns that have not been addressed by this policy, students, staff, parents and others are urged to seek clarification before carrying out any activities with ICT equipment.