COLLEGE INTERNET POLICY

[RE: electronic devices (eg notebook computers, mobile phones etc) and services – including cybersafety expectations]

Latest Update: May 2009

POLICY STATEMENT

The use of electronic devices and access to e-mail and internet services (school devices and services) in Catholic Education Office (CEO) Sydney schools are provided to students in order to support their educational and administrative needs. These school devices and services are necessary educational tools and **must be used in a responsible manner**. This policy can never anticipate all possible advances and uses of technology and therefore students who are unsure about their usage should seek clarification from the ICT manager as soon as possible.

This Policy is intended to inform parents and students of **the school's expectations when students are using the devices and services provided by the school and when using their personal equipment to communicate to or about members of the school community**. If a student acts in a way that is against the contents of the policy, he or she will be subject to consequences according to the College's Student Management Policy, and if necessary, offending material may be supplied to the police at the discretion of the Principal.

The school reserves the right to capture, store and review all internet browsing and email across the school network. Devices may be taken or accessed if it is believed that:

- **There has been or may be a breach of the school rules or policy**
- **There may be a threat of harm to a student or others or system security.**

RESPONSIBILITIES FOR STUDENTS ISSUED WITH SCHOOL OWNED NOTEBOOK COMPUTERS

(Refer to the Good Samaritan Catholic College Student and Parent Notebook Computer Guidelines)

The Federal Government has funded Good Samaritan Catholic College to purchase laptop computers for the personal educational use of year 9 students in 2009 while enrolled at the College. Students and their families who receive a laptop computer have the following additional responsibilities:

- To care for the notebook computer
- To keep the notebook computer secure, and protect it from any malicious damage
- To bring the notebook computer to school each day in readiness for use in the classroom – this includes having the battery charged and electronic files effectively managed
- **To replace or repair any damaged, lost or stolen notebook computer at their own cost**
- To return the notebook computer (and any inclusions such as power cords, USB HDD and carry case) in good order when leaving the school.

CYBERSAFETY REQUIREMENTS

This policy addresses the particular use of these technologies that has come to be referred to as **'Cyberbullying'** (See No. 4 below). The school will investigate and take action where this kind of bullying occurs in school **and** outside of school when it causes significant harm to the relationships between students and or teachers, or is criminal in nature.

1. When using the school devices and services **students will**:

- ensure that communication through internet and email services is related to learning.
- keep passwords confidential, and change them when prompted, or when known by another user.
- use passwords that are not obvious or easily guessed.
- log off at the end of each session to ensure that nobody else can use their e-learning account.
- promptly tell their teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
- seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
- ensure that copyright permission is gained before electronically publishing the works or drawings of others.
- Always acknowledge the creator or author of any material published.
- keep personal information including names, addresses, photographs, credit card details and telephone numbers, of themselves or others, private.
- ensure that school services are not used for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

2. When using school services or personal mobile phones, cameras, wireless devices or similar personal equipment **(when specific permission is given), students will not:**

- disable settings for virus protection, spam and filtering that have been applied by the school and not attempt to evade them through use of proxy sites.
- allow others to use their personal accounts.
- deliberately use the electronic identity of another person to send messages to others or for any other purposes.
- enter 'chat' or 'social networking' internet sites without the permission of a teacher.
- use unauthorised programs or intentionally download unauthorised software, graphics or music that are not associated with the learning activity as directed by a staff member.
- damage or disable computers, computer systems or networks.
- disclose personal information about another person (including name, address, photos, phone numbers)
- distribute or use information which is copyrighted without proper permission.
- take photos, video or audio recordings of members of the school community without their consent.

The school will not be responsible for lost, stolen or damaged personal equipment.

3. When using school services, **students will never knowingly** initiate or forward emails or other messages containing:

- a message that was sent to them in confidence.
- a computer virus or attachment that is capable of damaging recipients' computers.
- chain letters and hoax emails.
- spam, eg unsolicited advertising material.

4. When using school services or non school services **students will never** send or publish either through internet sites, e-mail or mobile phone messages:

- unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
- threatening, bullying or harassing material or make unreasonable demands.
- sexually explicit or sexually suggestive material or correspondence.
- false or defamatory information about a person or organisation.
- the school name, a staff members name or crest without the written permission of the Principal.

If a case of cyberbullying affects a student outside of school, the following course of action should be taken:

- The student immediately informs his/her parents/carers.
- The abuse is reported to the website owner or webmaster.
- If the concern is considered very serious, then the police should be informed immediately.

NETWORK ACCESS

1. Privileges

The use of Good Samaritan Catholic College's network is a privilege, not a right. Inappropriate use can result in a cancellation of those privileges. Based upon the acceptable use guidelines, the system administrators will deem what is inappropriate use of the network and take appropriate action. The system administrators or Principal may suspend or close an account at any time as required. The administration, faculty and staff of Good Samaritan Catholic College may also request the system administrator or Principal to deny, revoke or suspend specific user accounts.

2. Security

Security on any computer system is a high priority, especially when the system involves many users. If a student feels they can identify a security problem on the Good Samaritan Catholic College network, the student must notify the system administrator. They must not demonstrate the problem to other users.

Users may not, under any circumstances, use another individual's account. Passwords are not to be given to any other individual. Attempts to log in to the system as any other user may result in suspension or cancellation of user privileges.

Attempts to log onto Good Samaritan Catholic College's network as a system administrator will result in cancellation of all user privileges. Any user identified as a security risk or having a history of interfering with other computer systems may be permanently denied access to Good Samaritan Catholic College's network.

3. Vandalism

Deliberate vandalism will result in cancellation of privileges. Vandalism is defined as any attempt to obtain, harm or destroy data of another user, myInternet, or any of the above listed agencies or other networks that are connected to the Internet backbone. This includes, but is not limited to, the uploading or creation of computer viruses.

4. Reliability

Good Samaritan Catholic College makes no warranties of any kind, whether expressed or implied, for the service it is providing. Good Samaritan Catholic College will not be responsible for any damages students suffer. This includes loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by its own negligence or student's errors or omissions.

Use of any information obtained or given via myInternet is at a student's own risk. Good Samaritan Catholic College cannot guarantee the security of any personal information such as credit card details, or phone numbers, submitted via the internet. The College accepts no responsibility for any misuse of this information as a result.

While every endeavour is made to present accurate and up-to-date information, Good Samaritan Catholic College specifically denies any responsibility for the accuracy or quality of information obtained through its services.

All students are expected to sign a student contract which outlines responsibilities in relation to the College computer network and the internet.

Students need to be aware that all use of internet and email services can be monitored and traced to the accounts of specific users.

The misuse of school services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

Policy Update

This policy will be updated as necessary. All attempts will be made to adhere to the above policy, but particular circumstances (such as technological advancements) may require the Principal to depart from the stated policy.