Mount Evelyn Christian School
135 York Road
Mount Evelyn VIC 3796
ABN 19 775 686 269

Tel (03) 9738 6000
Fax (03) 9738 6001
office@mecs.vic.edu.au
www.mecs.vic.edu.au

Student Use of Information and Communications Technology Policy

The 'Student Use of ICT' Policy sets out the rights and responsibilities for computer and communications network users at Mount Evelyn Christian School. It covers use of the computer network and devices as well as e-mail and Internet facilities.

PREAMBLE

As a community of Christians we seek to be role models of Jesus and engage in the faith expressions of the community. Although as humans in a fallen world we are just as prone to sin as others are, nevertheless we pursue a life that is pleasing to God. Information and communication technologies (ICT) are an area of the creation in which we must be particularly wise since the possibility for misuse, sinful use, is significant and profound. Conversely, the opportunity that ICT offers for learning about God's world is also significant. Our values for ICT are:

- ICT is a part of our created world that should be subjected to a biblical framework of understanding.
- Students use ICT as a powerful set of tools to probe, think, question and learn. They should become wise in the use of these tools.
- Students use ICT as a powerful set of tools to communicate, collaborate, and demonstrate their learning. They should become effective users of these tools.
- ICT is not taught for the sake of ICT, and it is not taught merely that students gain vocational skills.
- ICT as a part of creation is also liable to the effects of sin. Students must become aware of how ICT may become a tool for harm, and what they can do to safeguard against and resist such uses.
- ICT is only one part of creation therefore we embed ICT learning throughout all areas of the curriculum. We also take time to teach specific ICT skills to ensure that the learning of such skills does not interfere with other learning.
- ICT resources and support are implemented according to a strategic plan that keeps our technologies current while taking account of prudent use of finances.

RATIONALE

This Policy sets out the rights and responsibilities for computer and communications network users at Mount Evelyn Christian School. It covers use of all ICT facilities.

POLICY SUMMARY

Mount Evelyn Christian School allows students access to its ICT resources. Access is governed by general principles of use, along with uses that are acceptable and unacceptable. This policy outlines these matters.

IMPLEMENTATION

GENERAL PRINCIPLES

To serve the curriculum, Mount Evelyn Christian School allows students access to certain ICT resources. These include school computers and devices, Internet, email, networks and intranets. Some of the general principles for use include:

- Use of computers and online facilities are for educational purposes.
- Student access to the ICT resources is dependent on standards of behaviour.
- We expect students to be responsible and mature in their use of the computer facilities and network at all times.
- Students must understand that their access to the school's computer facilities and network will only be allowed for acceptable and ethical purposes.
    - What is 'Acceptable' is outlined in Sections 2 and 3 of this Policy.
    - 'Ethical' means that students are not allowed to breach standards of common decency, or manners, and must not break any laws.
- Students who use computer facilities and network irresponsibly or unethically will be disciplined.

STUDENTS' RESPONSIBILTIES

SECTION 1: ACCESS TO THE COMPUTER FACILITES

Users are expected to use the school's computer network system to further educational goals. Students must be familiar with the school's guidelines for computer use. We manage this as follows:

- Students are given access initially at the start of the year and must complete this process by the due date to retain access.
- Each year, Primary School students must, in conjunction with their parent(s), read and sign the relevant Primary School Student ICT Use Agreement.
- Each year, Middle and Senior School students must, in conjunction with their parent(s), read the Student Use of ICT Policy (this document) as well as read and sign the Secondary School Student ICT Use Agreement.
- Students return their signed agreement to the school by the due date. This "signing" may take printed form or may be indicated via an online agreement If this is not completed by the due date, access will be revoked.

Access to computer resources is controlled by using usernames and passwords. Students choose a password that is no less than 8 characters and should be easy to remember but complex enough not to be guessed. Prep and Junior Primary students will be assigned a password.

SECTION 2: ACCEPTABLE USES

1. Students can use school computers, send and receive e-mail and use the Internet for educational purposes as directed by staff.
2. Students should use these resources as efficiently as possible. Before downloading or printing anything, thoughtful consideration should be given as to whether this is really necessary. Students should not be wasteful and should exercise good stewardship of these resources as well as considering any environmental impact. If unsure, a teacher should be consulted.

SECTION 3: UNACCEPTABLE USES

The following examples are guidelines for the types of uses that students must not be involved in. The school may determine that other forms of behaviour not listed below are unacceptable.

CONCERNING THEMSELVES

Students must **not**:

1. Use a username or password other than their own or disclose their password to another person.
2. Give out any personal details about themselves, family or friends. That includes names, address, telephone number(s), email address(es), photographs, school's name, gender, date of birth or age.
3. Arrange a meeting in person with someone they have 'met' on the Internet.
4. Not web 'surf' without an educational purpose.
5. Use the computers to play non-educational games.
6. Upload or download any software without staff permission.
7. Use or download 'peer to peer' software.
8. Use any social networking or chat programs.
9. Access, download, store, print or distribute pornographic, obscene or violent material.
10. Respond to email messages that are indecent, suggestive, belligerent, discriminatory, threatening, or which make the student feel uncomfortable or unsafe in any way.
11. Use the school facilities for commercial or profit-making exercises or purchase goods or services via the school.

CONCERNING OTHERS

Students must **not**:

12. Harass, be impolite, abusive or discriminate against others.
13. Disclose any personal detail of any other person.
14. Knowingly write false or defamatory information about a person or organisation or falsify a communication so that it appears to be from another person or organisation.
15. Breach another person's or organisation's copyright by downloading, using, printing or saving to file without permission. This includes music, videos, images or other pirated software.

CONCERNING THE SCHOOL SYSTEM

Students must **not**:

16. Attempt to gain unauthorised access to any network i.e. hacking.
17. Attempt to disrupt the use of computer and network facilities by: deliberately damaging equipment, spreading computer viruses, connecting faulty devices, or by any other means.
18. Deliberately tamper with or modify any hardware or software, or change the set-up of any software or computer.
19. Attempt to connect an unauthorised device to the school network.

SECTION 4: PENALTIES FOR MISUSE OF THE COMPUTER NETWORK

Mount Evelyn Christian School has the responsibility to enforce this policy and discipline those students who breach it.
We expect students to honour the agreement they have signed. If, in the school's opinion, a student has used the computer facilities and network for an unacceptable purpose, unethically or otherwise inappropriately, at the very least the student will lose the privilege of access for a period of time determined by the school. In most cases parents will be notified.
Depending upon the seriousness of the student's actions, other penalties may be considered, including but not limited to:

- Suspension and expulsion.
- Police notification - Students should be aware that the school will advise and cooperate with the police and other authorities in any investigation relating to the illegal uses of the computer facilities and network.

SECTION 5: NETWORK PRIVACY AND SECURITY ISSUES

Students should be aware that their electronic communication and work created via the school's computer facilities and network is not private, and in order to comply with its obligations under law, the school reserves the right to access students' files, work and electronic communications to ensure that the computer facilities and network are being used for acceptable purposes and in accordance with this Policy. This extends to files in connection with their curriculum, incoming and outgoing e-mail communications and sites accessed on the Internet.
In addition, the school's system administrators, as part of normal monitoring procedures, may access students' files. 'Normal monitoring' includes spot checks to ensure that inappropriate material, or work subject to another person's copyright, is not being kept in private folders and inappropriate Internet sites have not been visited.

SECTION 6: LIMITATION OF LIABILITY

Students will be allowed access to the computer facilities and the network as for their learning. It is not practical that every student will be supervised individually when using the computer facilities and network, and the school expects students to act responsibly and sensibly when using the computer network. The school does not accept any liability, financial or legal or otherwise, that may result from any student's unacceptable or unethical uses of the computer facilities, network or Internet connection.