



MERCEDES COLLEGE

COMPASSION LOYALTY JUSTICE INTEGRITY RESPONSIBILITY MUTUAL RESPECT

Technology Acceptable Use Policy

Preamble

Mercedes College provides a significant level of information and communications technology (ICT) in order to enhance learning and contribute to the academic and social development of the community. The primary purpose of ICT at Mercedes College is to promote educational excellence by facilitating resource sharing, innovation and communication.

ICT includes the provision of hardware, software and access to the Internet. The Internet is a global network that enables access to a wide range of information sources and communication opportunities including email. Email is neither private nor secret. It may be easily copied, forwarded, saved, intercepted, archived and may be subject to discovery in litigation. The audience of an inappropriate comment in an email may be unintended and extremely widespread.

This policy covers the utilization of any equipment, property or resource at any time, whether during or outside of school hours, and includes the use of remote access facilities. Further, this policy also applies to the use of personal devices accessing the College's resources.

Rationale

The intent of this Policy is to establish the rules for governing safe and legitimate use of information and communications technology (ICT) at Mercedes College. And to ensure ICT is used in harmony with the Catholic ethos of the College and in keeping with Mercy tradition. Users must be familiar with the terms of this Policy and will be required to sign an Acceptable Use Agreement in relation to their responsibilities.

Principles

This Policy is based on the Mercedes College Vision to “develop global citizens, committed to living with compassion, loyalty, justice, integrity, responsibility and mutual respect” and the key principle of “supporting a positive learning environment”.

Policy Statement – Use of ICT

The College's computer network and other communication facilities are educational and business facilities provided by the College to be used primarily for educational purposes. All users, therefore, have a responsibility to use these resources in an appropriate, ethical, safe and lawful manner.

Authorised users are permitted to access the Internet, email and other communication facilities to send and receive personal messages, provided that such use is consistent with user responsibilities as outlined in this Policy. Individuals are liable for what is written or said in an email or other communication message.

Text (including song lyrics), computer programmes, illustrations (including maps and diagrams), photographs, recordings, films and television broadcasts are all protected by the Copyright Act (1968). Users are to respect the rights of copyright owners.

The Commonwealth Privacy Act (1988) requires individuals and the College to take reasonable steps to protect the personal information that is held from misuse and unauthorized access. Further, the Commonwealth Privacy Act (1988) prohibits the use of photographs or other forms of illustration that may identify an individual without their direct consent. This includes (but is not limited to) the use of digital cameras and mobile telephones to record and transfer images.

Policy Statement – Use of Mobile Phones

Mercedes College does not prohibit students from bringing personal mobile phones to school. However, there is a distinction between the use of mobile phones as a personal communication device and as an educational (ICT) device.

As a personal communication device, students are not permitted to use their own phones at any time during the school day, between 8.30am and 3.30pm. If any student needs to use his/her phone during these hours, permission needs to be first obtained from a member of the teaching staff.

As an educational device, students are expected to follow the guidelines relating to ICT use outlined in this Policy under the direction of teaching staff.

Policy Statement – Consequence of Breach

Breaches in the conditions of this Policy will be investigated by the Executive Leadership Team to determine disciplinary action which, depending on the extent of the misconduct, may include dismissal or prosecution for a criminal offence.

Policy Statement - Limitation of liability

Mercedes College does not guarantee that the functions or services provided by or through information and communications technology will be error-free or without defect.

- Mercedes College will not be responsible for any damage students may suffer including, but not limited to, loss of data or interruptions of service, whether or not such loss of data or interruptions of service is incurred through a breach of this Policy.
- Mercedes College is not responsible for the accuracy or quality of the information obtained through or stored on the network.
- Mercedes College will not be responsible for financial obligations arising through the unauthorized use of provided technology.

Procedural Understandings

1. Use of the Mercedes College ICT Resources

- 1.1 All documents created and stored on the network will be treated as education related. Accordingly, users should not expect that any information or document transmitted or stored on the computer network is private.
- 1.2 The College's facilities and communication technology should not be used for the conduct of a private business.
- 1.3 Users are not to download or post material that could cause damage or disruption. This includes, but is not limited to, viruses and instructions on creating explosive devices.
- 1.4 Users are not to download or forward games, audio clips, movie clips or other files that do not constitute educational purposes. The downloading and installing of music sharing software is strictly prohibited.
- 1.5 Authorised users are not to interfere with another person's ability to undertake their responsibilities or duties.
- 1.6 Authorised users have a limited amount of space on the network to store files. Any files that are no longer required should be transferred to storage devices or removed from the network.

- 1.7 The use of printers, scanners, digital cameras, projectors and other technologies available at the College is limited to activities of educational or career development purposes.
- 1.8 The use of storage devices such as (but not limited to) floppy disks, CD's, DVD's and USB drives are for storage and transfer of files related to educational purposes.

2. Internet Access and Electronic Mail

- 2.1 Email addresses for authorised users are in the form of username@mercedes.catholic.edu.au
- 2.2 The Internet, email or messaging should never be used for the following purposes:
- (a) To abuse, vilify, defame, harass, degrade or discriminate (on the grounds of, for example, sex, race or disability etc.) Defamation refers to any statement (including photographs and cartoons) that can harm another person's reputation. The use of mobile telephones with image capabilities may constitute a case for defamation (see also Privacy).
 - (b) To send, assent to receive or store obscene, offensive or pornographic material;
 - (c) To discuss or comment on the physical appearance of other persons (whether they receive the message or not);
 - (d) To harass any person whether through language, frequency or size of message;
 - (e) To injure the reputation of the College and/or the Church in a manner that may cause embarrassment to any member of the College community or the Church;
 - (f) To offend the ethos and values of the Catholic teachings;
 - (g) To send unsolicited mail to multiple people (spam);
 - (h) To send anonymous email intended to disguise one's identity or origin;
 - (g) To infringe the copyright or other intellectual property rights of another person (see Plagiarism and Copyright);
 - (i) To deliberately access or remain at a site with inappropriate or offensive content. From time to time users may be redirected to, or accidentally access, inappropriate material. These sites should be brought to the attention of the Systems Administrator or Head of School in order for them to be blocked by the College's filtering software and to ensure that it is noted that the material was not accessed intentionally.
 - (k) To perform any other unlawful or inappropriate act.
 - (l) To post messages using social networking sites unless the message is strictly related to education or College business.
- 2.3 Users must regularly check their email and delete and trash unwanted messages promptly. Email is regularly cleared by the network system after certain time periods have elapsed.
- ## **3. Plagiarism and Copyright**
- 3.1 Information found on the Internet or on the College network cannot be used or distributed without the right to do so. Plagiarism is taking the ideas or writings of others and presenting them as if they were your own. Users must check that there is no violation of intellectual property rights. Proper referencing of material is required.
- 3.2 Users are to respect the rights of copyright owners. Copyright infringement occurs when you inappropriately reproduce a work that is protected by copyright. If a work contains guidelines for appropriate use of that work, then users must follow the express requirements.

- 3.3 Users should assume that all materials published on the Web are copyright, unless explicitly stated otherwise. If a user wishes to use material from another webpage in one of their own pages, then they should create a hyperlink pointing to the material rather than copy it. It is recommended that the permission of the owner of the other web page be sought prior to creating links to their pages
- 3.4 A user must not copy a trademark or logo belonging to another party. This constitutes a breach of the Trade Marks Act (1955) and will expose the user to liability for damages. By including these logos on a Mercedes College web page, this may also breach the Trade Practices Act (1974) by deceptive or misleading conduct.
- 3.5 Software must not be copied without the express permission of the copyright owner. Authorised users must respect and abide by the terms and conditions of software use and licences.
- 4. Privacy**
- 4.1 Users are forbidden to post personal contact information about themselves or others including staff, students and parents.
- 4.2 The Privacy Act requires individuals and the College to take reasonable steps to protect the personal information that is held from misuse and unauthorised access. When logged on, each user is responsible for the security of the computer and should not allow it to be used by an authorised user.
- 4.3 Intentionally seeking information, obtaining copies or modifying files or representing others without express authority is prohibited.
- 4.4 The Privacy Act prohibits the use of photographs or other forms of illustration that may identify an individual without their direct consent. This includes (but is not limited to) the use of digital cameras and mobile telephones to record and transfer images.

Monitoring ICT Acceptable Use

- Mercedes College has established procedures to assist in the provision of information technology services and the maintenance of security. This includes the use of network accounts and passwords to restrict access to the network to authorised use only.
- The contents and usage of email and Internet access may be subject to regular random monitoring by the College. This will include electronic communications which are sent or received, both internally and externally. Where inappropriate use is suspected through this means or other incidents, the Systems Administrator may be authorized by the Heads of Schools or Principal to examine web access logs and/or email accounts. No monitoring will occur without this authority except for normal logging of system usage to manage the network.

Consequence for Policy Breaches

Any user found breaching the conditions of this Policy will have their access to ICT resources removed for a minimum two week period. This may involve a number of options including disabling network access or banning the use of personal devices. During this time the relevant Head of School will investigate the breach to determine if more severe consequences are required. Only the Head of School can authorize restoration of access. While access is restricted, the user is not permitted to use another person's access.