MARIST COLLEGE ASHGROVE
A Catholic boys' day and boarding College in the Marist Tradition

Acceptable Use of Technology (Student)

ITEM	DESCRIPTION
Policy description	This policy outlines the procedures for the acceptable use of technology for students.
Department	Information Technology
Executive Director	Deputy Headmaster
Contact	Deputy Headmaster Ph: 07 3858 4555
Date approved	1 January, 2020
Next review	1 January, 2021

Revision History

DATE	VERSION	REVIEWED BY	CHANGES MADE
Date of first revision Date of second revision Date closed			

Printed copies of this document may not be up to date. Ensure you have the latest version before using this document.

Table of Contents

1. The Hazard - Information and Communication Technology

Information and Communication Technology (ICT) includes any electronic device or application used to communicate, create, disseminate, store or manage information such as text, images, audio or video. Examples include:

- Personal computers and laptops;
- Mobile devices such as mobile phones and tablets;
- Applications such as email, social networking apps and the internet;
- Web-based tools such as social networking sites, chat rooms, blogs, podcasts and instant messaging systems;
- Imaging tools such as video, still or web cameras and related software;
- Audio tools such as audio recording devices, iPods, mp3 players and related software; and
- Fax, scanning and copying machines.

The Acceptable Use of Technology policy covers College devices as well as student owned devices when used for College purposes.

Access to the internet, email and other network services is provided by Marist College Ashgrove as a service and educative tool to students and to enrich teaching and learning at the College. This access is granted with expectations regarding the use of devices and services for learning.

2. Marist College Ashgrove's Policy

Students have the right to learn in a safe environment, including when they have access to ICTs to enhance their learning. Marist College Ashgrove is committed to the responsible and educational use of ICTs and to the protection of students by providing secure access to these services as part of their learning experience.

It is our policy that:

- The use of ICTs be managed through a 'whole of College community' approach involving students, staff and parents/carers;
- ICT education strategies be implemented within the College on a continuous basis with a focus on teaching age appropriate skills and strategies to empower staff, students and parents/carers to ensure appropriate use;
- Staff are positive role models in use of ICTs;
- All Staff and Students use ICT in an appropriate manner at all times; and
- Our ICT policy is reviewed on an annual basis against best practice.

3. Emails

Personal emails can easily be forwarded to other parties for whom they were not originally intended and the message manipulated or misconstrued. This may result in the liability of the sender for various matters including sexual harassment, defamation or discrimination.

It is important to remember that emails are neither private nor secret. They are discoverable documents that may be required to be produced in legal proceedings.

Students should not expect that any information or file transmitted or stored on the College's network will be private or kept confidential.

4. Student Owned Devices (tablets, personal laptop computers, media players, cameras, etc).

As part of the College Technology Plan, students are permitted to bring technological devices to support their learning.

Students must comply with the Acceptable Use of Technology conditions when student owned devices are used for College purposes.

Inappropriate use of student devices will result in the device being confiscated and the student will need to collect it from Student Administration or Head of House at the conclusion of the day and an appropriate consequence will occur at the time. Confiscated media devices may be handed to the Police if the law is suspected to have been broken.

The College permits students to connect devices to the Internet through a wireless network for educational purposes only. Conditions for the use of the Internet, email and other network services apply to personal devices when connected to the College's wireless network.

The College accepts no responsibility for the loss, theft, unauthorised use or damage of any student owned computer, tablet, mobile phone, media player or other personal device.

5. Mobile Phones

The College recognises that students having access to a mobile telephone device provides some parents peace of mind, enables emergency arrangements to be made conveniently and, in some instances, provides increased safety for students.

Mobile phones can create a range of hazards when brought to school, such as:

- Students taking video footage or photos of people without their permission,
- Providing an increased risk of theft, loss or damage,
- Temptation for cheating during exams,
- Using phones inappropriately to bully, intimidate or harass other students or staff. This can have serious consequences including police involvement, and
- Possible disruption to assemblies, classroom learning and/or religious services for both the user and fellow students.

Students at Marist College Ashgrove are permitted to bring mobile phones to school however it is College policy that they are not to be accessed or visible during the hours of 8.30am-3.10pm. Should a student need to use their mobile phone they may do so either in their respective Head of House's office or Student Administration.

Students found to be accessing their mobile phones during the hours of 8.30am-3.10pm outside of the permitted areas (Student Administration/Heads of House offices) will have

their mobile phones confiscated for the remainder of the day. It will then be the responsibility of the student to collect their mobile phone from Student Administration prior to leaving school that day. Second and subsequent infringements will also result in further consequences being imposed.

Mobile phones must not be taken into examinations.

For further information regarding student use of mobile phones refer to the College Mobile Phones (Student Use of) policy.

6. Student Responsibilities

Students will:

- Use ICT devices and systems for learning not for games and entertainment;
- Use electronic devices in accordance with teachers' or staff members' instructions, both in the classroom and on school grounds;
- Keep their device secure. Passwords must not be shared. Security is the student's responsibility.
- Access to the Internet is through the College's WiFi only, not 3G or 4G;
- Obtain permission from a member of the CLT before photographing, videoing or sharing online;
- Ensure the device is fully charged each day'
- Clearly label their device(s);
- Regularly backup important work. Students are responsible for their own data;
- Interact with others appropriately, responsibly and respectfully; and
- Report any security concerns to the IT Helpdesk immediately.

Students must ensure they do not:

- Publish or share any images containing the College crest, uniform or grounds without permission from a member of the College Leadership Team.
- Use Internet or network access inappropriately to:
  - ⇒ Access any online content or other online spaces that would be considered offensive because of pornographic, racist, violent, illegal, illicit or other inappropriate content;
  - ⇒ Use obscene, harassing or abusive language;
  - ⇒ Violate copyright laws by posting or distributing copyrighted material by illegally downloading software, games, music, graphics, videos or text materials;
  - ⇒ Attempt to change settings and preferences which have been protected by an administrator;
  - ⇒ Use another person's data, online accounts or view their information without permission;
  - ⇒ Share passwords with other students; and
  - ⇒ Cause embarrassment or loss of reputation to the College, or be unjustifiably critical of the College, its students or employees

- Bypass security settings to:
  - ⇒ Attempt to obtain unauthorised access to the College or any other computer system or data stored in any computer system; and
  - ⇒ Attempt to probe security mechanisms at the College or any other Internet sites.
- Damage or interfere with College computer or network equipment.

7. Parent Responsibilities

Parents should support the College by monitoring appropriate internet access by their student, in their home and ensure students understand the importance of not sharing their passwords with other users.

8. Viruses

Students have a responsibility to ensure that any material obtained from other sources is checked for infection by viruses, prior to its use on the College network.

Students who suspect that a file or document including an email attachment may have a virus are advised to:

- Avoid opening the file;
- Delete the attachment, file, document; and
- Seek support from the College Computer Support Team.

9. Monitoring and Privacy

Marist College Ashgrove reserves the right to monitor and log internet usage, including email, to ensure:

- The integrity of the network is maintained;
- The network is not being used for authorised, lawful activities; and
- The network is being used consistently with these guidelines.

Such situations may include:

- The need to access files when the person responsible for that information is unavailable; or
- The College suspects that there is unlawful or unethical use of the network, or where there has been a suspected breach of these conditions.

Students should comply with all relevant state and federal privacy legislation when using information collected and stored on the computer network.

10. Breaches

Student breaches of the above conditions would constitute unacceptable use. Measures likely to follow a breach include, but are not limited, to:

- Discussing appropriate usage;
- Temporarily or permanently revoking email and/or internet usage;
- Limited and/or managed use of device or confiscation; and
- Disciplinary action, including possible suspension or exclusion

11. ICT Misuse Prevention Strategies

Marist College Ashgrove recognises that the implementation of whole of College prevention strategies is the most effective way of eliminating, or at least minimising incidents of misuse of ICTs within our community.

The following initiatives form part of our overall ICT strategy:

- A structured curriculum and peer group support system, that provides age appropriate information and skills relating to ICT use to students over the course of the academic year;
- Education, training and professional development of staff in appropriate ICT use;
- The regular provision of information to parents/carers to raise awareness of inappropriate use of ICTs as a College community issue;
- The promotion of a supportive environment that encourages the development of positive relationships and communication between staff, students and parents/carers;
- All student login details and passwords are to be kept confidential to prevent others accessing their accounts;
- Access to College networks is provided through a filtered service. The filter is designed to restrict access of inappropriate material as well as providing spam and virus protection;
- Approval must be sought before connecting privately owned ICT equipment and devices to College networks to avoid the risk of malware;
- Students are required to sign and abide by Marist College Ashgrove's Information and Communication Technology Use Agreements which specify details of inappropriate usage. No student may use College owned ICT equipment and devices unless the agreement has been signed and returned to the College. All signed agreements will be kept on file at the College;
- Inappropriate usage by students includes:
  - ⇒ Participation in non-educational activities such as the purchase and/or sale of products or services;
  - ⇒ Illegal activities such as threatening the safety of others or engaging in criminal activity;
  - ⇒ Tampering with or damaging computer hardware or software; and
  - ⇒ Making, installing or downloading copies of software that is not licensed by the College.
- Any inappropriate internet sites accidentally accessed, incidents where students are offended by another person's use of ICTs and suspected technical security breaches must be immediately reported for investigation;
- Appropriate copyright clearance is sought and the source of any information used or published is acknowledged, to avoid plagiarism;
- The College reserves the right to monitor, traffic and review all content sent and received on the College systems;
- Breaches of acceptable usage of ICTs will result in disciplinary action;
- Regular risk assessments of inappropriate ICT use within the College;

- Records of reported incidents of ICT misuse are maintained and analysed in order to identify persistent offenders and to implement targeted prevention strategies where appropriate;
- Statements supporting appropriate ICT use are included in students' College diaries; and
- Posters promoting appropriate ICT use are displayed strategically within the College.

12. Workers' Responsibility

All workers are responsible to:

- Model appropriate behaviour at all times;
- Ensure all students are provided with ICT Agreements, that they understand them, and that they understand they will face disciplinary action in the event they misuse ICT equipment and devices;
- Ensure that students who do not return their ICT Agreements do not use ICT equipment and devices;
- Be vigilant in monitoring students when using ICT equipment and devices;
- Reinforce to students the importance of privacy and safeguarding their login details, personal information and the personal information of others;
- Assist students in the event that they have inadvertently accessed inappropriate material, received inappropriate messages or if they have been offended by another person's use of ICTs;
- Deal with all reported and observed incidents of inappropriate ICT use in accordance with this policy; and
- Ensure that any incident of inappropriate ICT use that they observe or is reported to them, is recorded appropriately.

13. Implementation

This policy is implemented through a combination of:

- Staff training;
- Student and parent/carer education and information;
- Student ICT Agreements;
- Signage promoting appropriate ICT usage;
- Effective student supervision;
- Effective supervision and monitoring of College networks;
- Regular inspection of ICT equipment;
- Effective incident reporting procedures;
- Effective management of incidents of inappropriate ICT usage when reported and/or observed;
- Regular risk assessments with respect to inappropriate ICT usage;
- Effective record keeping procedures; and
- Initiation of corrective actions where necessary.