



# ICT Acceptable Use Agreement Policy

## Rationale:

At Catherine McAuley College, as a Mercy School living in the Spirit of Catherine McAuley and following the model of Jesus are dedicated to our Touchstone Statement.

'Inspiring members of our community to be learners impelled to thrive and serve'

The College supports the rights of all members of the College community to be provided with and engage in a safe, inclusive and supportive learning environment. This extends to the use of digital tools and online communities and is underpinned by our expectation of safe and responsible behaviour of all members of the College community.

This document outlines the rights and responsibilities of the Catherine McAuley College (CMC) community in relation to the use of College computer equipment and facilities.

## Definition:

*This policy applies to:*

- **Students:** All enrolled students of Catherine McAuley College
- **Staff:** All Catherine McAuley College staff including teachers and support staff
- **Parents/Carers:** Includes the natural biological parents, carers or legal guardians of a student
- **Computer 1:1 Program:** The term one-to-one is applied to programs that provide all students with their own laptop (one-to-one refers to one laptop per student)

## Policy Statement:

*It is the policy of Catherine McAuley College:*

CMC provides all students' access to the computer 1:1 program at CMC.

At CMC:

- There is a Student Code of Conduct that states our College's values and expected standards of online behaviour, including actions and consequences for inappropriate online behaviour.
- We educate our students to be safe and responsible users of digital technologies.
- Raise our students' awareness of issues such as online privacy, intellectual property and copyright.
- Supervise and support students when using digital technologies within the classroom and establish clear protocols and procedures when working in online spaces including reviewing and considering the safety and appropriateness of online tools and communities:
  - [Bullystoppers Duty of Care and Supervision](#)
- Provide a filtered internet service but acknowledge that full protection from inappropriate content can never be guaranteed.

- Respond to issues or incidents that have the potential to impact on the wellbeing of our students including those reported through online services.
- Know that some online activities are illegal and as such we are required to report this to the appropriate authority.
- Support Parents/Carers to understand the safe and responsible use of digital technologies, potential issues and the strategies that they can implement at home to support their child providing this ICT Acceptable Use Agreement and current information from both the Department of Education and Training and Cybersmart:
  - [Bullystoppers Parent Interactive Learning Modules](#)
  - [Parents Cybersafety guide](#)

## 1.1 Agreement

Access to the College's computer facilities is provided to support the College's learning and teaching objectives. Student use of these tools is subject to this policy, other than relevant College policies, ethical standards, CEO or CECV policies and procedures and government regulations.

Each individual using the College network agrees that they are responsible for their actions. Users understand that all aspects of the use of Information Communication and Technology (ICT) at the College can be monitored or logged. Any breach of conditions could result in the student's accounts being suspended or other disciplinary action as determined by the College's disciplinary structures.

By using the College network and services, students agree to accept the conditions outlined in this document.

## 1.2 General Conditions

All users agree to:

- Respect others and communicate with them in a supportive manner; never writing or participating in online bullying (including forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviours).
- Protect their privacy, not giving out personal details, including full name, private telephone number, address, passwords and images.
- Protect the privacy of others, never posting or forwarding their personal details or images without consent.
- Talk to a teacher or trusted adult if they personally feel unsafe or uncomfortable online or if they see others participating in unsafe, inappropriate or hurtful online behaviour.
- Carefully consider the content that they upload or post online, knowing that this is a personal reflection of "who I am and what people think of me".
- Handle ICT devices with respect and care (e.g. not eating or drinking whilst using a College computer and notifying ICT when there is any damage or attention required).
- Not deliberately seek to infect, damage or destroy hardware and/or software.
- Not use the computer to listen to music, watch videos, send messages or play games unless approval has been granted by the supervising teacher.
- Not use someone else's account or to allow someone else to use their account.
- Not transmit files or documents which covertly include malware or viruses. Students must take reasonable steps to ensure that they do not introduce or propagate computer virus infections within the College community.
- Not breach copyright laws.

- Not have unauthorised access (or attempt access) to any other person's computer, network account, email accounts or equipment.
- Not inappropriately access or attempt to access, College classified or personal information.
- Not connect any device to school computers other than a simple USB memory stick or external drive unless a staff member gives permission.
- Not save any non-schoolwork material (e.g. games, mp3 files, videos, programs, photos, etc.) onto the College network.
- Not disadvantage other users of the College's network by downloading or uploading large files or other data. Thus, the downloading or uploading of games, music, movies or any other data via the College's network, which is not directly related to a student's educational needs, is not allowed.

The understanding that those who chose to connect additional devices (mouse, headphones, speakers, etc.) do so at their discretion and the College accepts no responsibility for these devices. Such devices may only be used after approval by the staff member.

## **1.3 Facilities**

### **1.3.1 Internet Facilities**

All users agree not to:

- Publish material that brings the College, its staff or students is disrepute, or is defamatory.
- Be involved in any form of cyber bullying including the use of phones, social websites, game sites, email, internet chats or instant messaging.
- Use the internet in class time for recreational purposes unless permission has been granted by the supervising teacher.
- Use chat (IRC) sites or Instant Messaging programs within school unless approved by staff.
- Access or transmit any material that is offensive or obscene (e.g. violent, racist, sexist, pornographic) or in violation of any law or government regulation (e.g. equal opportunity regulations).
- Attempt any hacking activities.
- Attempt to bypass the College proxy in any way in order to connect to the internet.
- Disclose a network login password.

### **1.3.2 Email Facilities**

All users agree not to:

- Disclose their email password.
- Write messages that contain words or any material that are defamatory or inappropriate (e.g. violent, racist, sexist, pornographic) or in violation of any law or government regulation.
- Use language that is swearing or abbreviations of swearing.
- Read email messages of recipients other than their own.
- Send spam, annoying, harassing or abusive emails. This includes "chain" or "forward (fwd)" emails. Email is considered harassment if it offends the receiving party in any way.
- Answer unsolicited emails, quizzes or advertising questionnaires.
- Use the school email account for purposes other than education (e.g. exchanging files or information not relevant to school work).

- Send a message under someone else's name or a false name.

These lists should not be taken as exhaustive. The onus is on the individual where doubt exists to seek advice and clarification from relevant teaching or administration staff.

The emails system is the property of the College and as such is **not completely confidential and private**.

College email system administrators and/or other authorised persons may access email:

- When there is a reasonable basis to believe that a College policy or Federal, State or Local law has been violated. To diagnose and resolve technical problems

#### **1.3.2.1 Inappropriate Material**

Students who inadvertently encounter material that is inappropriate should bring the material to the attention of their teacher who will take appropriate action. Employees or Parents/Carers should bring the material to the attention of a Leadership Team member.

#### **1.3.3 Acceptable Use of Computer Facilities**

The College provides computers to facilitate teaching, learning, and communication. When using College computers, users are expected to:

- Use equipment only for school related activities unless approval has been granted by the supervising teacher.
- Maintain the Standard Operating Environment (SOE) – that is, do not substitute or modify the operating system, tamper with or remove College provided resources.
- Keep equipment clean and in good working order and report faulty or damaged equipment immediately.

This list should not be taken as exhaustive. Common sense, consideration for others and decency should determine the actions of users. The onus is on the individual where doubt exists to seek advice and clarification from relevant teaching or administration staff.

#### **1.4 One-to-One School Owned Devices**

- The laptop supplied to each student is College property and it is the responsibility of the student to take adequate care of the computer.
- When a student leaves the College, the computer must be returned to the College no later than the student's last day at the College.
- Students must bring the computer to school every day, ensuring that it has been fully charged overnight.
- For environmental reasons, students should refrain from printing unless it is absolutely necessary.
- When it is not in use during the school day the computer must be stored in the student's locked locker.
- Students are permitted to take the computer home.

- Students are not permitted to leave the computer overnight in a classroom or their locker.
- Backup of important files on the computer is the responsibility of the student. Students should maintain a backup of all schoolwork on an external device or cloud storage.
- Students are not permitted to bring privately owned computers to school unless:
  - There are extenuating circumstances which warrant the use of such and approval has been granted.
  - There are exceptional program requirements for a particular class and approval has been granted.
- Students are permitted to customize the device wallpaper, but in doing so must not infringe copyright nor offend any member of the College community.
- Students are permitted to have music files, photographs and movie files stored on their computer. It is essential that these files are legally owned. The copyright Act prohibits users from storing music/photographs/movies under copyright (owned by others). Students are not allowed to play music or movie files during class time unless permitted by the teacher.

## **1.5 Social Media**

The College understands that there is a great potential for the use of social media in school communities in terms of educational outcomes and as a means of communication. However, students must understand the expectation of the College when using social media in an educational and personal capacity.

Social media can only be used at school when directed by a staff member as part of a school activity.

### **1.5.1 Social Media Risks**

- Reputational damage to the College and Students.
- Disclosure of confidential information and breach of privacy laws.
- Posting of offensive, bullying, harassing and discriminatory material.
- Misuse of intellectual property and breach of copyright laws.

## **1.6 Viruses**

Everyone must take reasonable steps to ensure that they do not introduce or propagate virus infections within the College community. Such reasonable steps include:

- Verifying anti-virus program is running.
- Regularly scan any flash drives or other media used for transporting or distributing files.
- Not opening files from insecure sources or sources where security is unknown or questionable.
- Not opening emails that is of a questionable or of dubious origin.
- Only opening email attachments that are expected or from trusted sources.

## **1.7 Passwords**

Each student password must be secure. Passwords should be not easy to guess or hack. To facilitate this, the following guidelines should apply:

- No dictionary words or names of places, pets, people, etc.

- A minimum of 6 characters.
- At least three of the following:
  - Uppercase letters
  - Lowercase letters
  - Numbers
  - Special character (!@#\$%^&\*)
- Do not write down passwords or store on your computer.
- Never allow another person to watch you when you are entering a password.
- Members of the College community are expected to meet the requirements specified in the Network Password Policy.

### **1.8 Peripherals**

Students are welcome to connect home networks, home printers, digital cameras, scanners and other peripheral devices to their computer. Please remember that the College's ICT technicians cannot provide support for computer issues which occur at home.

### **1.9 Webcams/Voice Recorders**

Computers are equipped with a webcam and a voice recorder. These can be useful and powerful educational tools when used appropriately. However, students are only permitted to use these features of the computer at school if:

- They have the permission of their supervising teacher on each day and any occasion.
- They have the express consent of all individuals who will appear in any images, video or voice recordings created using these tools.
- They do not distribute or publish identifiable images or sound recordings of others beyond the College's network without first gaining the approval of the individual, a Parent/Carer and the classroom teacher.
- Images, videos or sound recordings do not portray anyone in a situation which is offensive, demeaning or defamatory.

### **1.10 Non-Compliance with this Agreement**

If the College considers that a student has in any way failed to comply with this policy, it may:

- Immediately remove the student's access to any part of the College's computer system.
- View all files held on the computer.
- Audit and view all material viewed on, sent to and from its computer system (including internet sites and email attachments).
- Re-image the computer.
- Take disciplinary measures against the student.

### **Duty of Care**

Catherine McAuley College is a Child Safe School. We owe all students a duty of care to take reasonable measures to protect them from risks of injury that should have been reasonably foreseen. All on and off-site activities require appropriate supervision and greater measures may need to be taken for younger students or students with disabilities to meet this duty of care. The College's risk assessment procedures and emergency management plan provide the processes for ensuring the above is achieved.

## Minimum Standards

The College monitors its compliance with the minimum standards in line with Ministerial Order 870 in an ongoing manner.

## Legislation:

This Policy is mandated by:

- The copyright Act 1968
- Education and Training Reform 2006
- Education and Training Reform Regulations 2007
- Education and Training Reform Amendment 2010
- Australian Education Act 2013
- Australian Education Regulation 2013
- Education and Training Reform Act – Child Safe Standards – Managing the Risk of Child Abuse in Schools, Ministerial Order No. 870
- Information Privacy Act 2000

## Related Policies, Procedures and Forms:

- Mobile Phone Policy
- Bullying, Discrimination and Harassment Policy
- Student Behaviour Expectations Policy
- ICT Backup and Recovery Policy
- Network Password Policy
- Catholic Education Sandhurst Limited - [Duty of Care Framework](#)
- Catholic Education Sandhurst Limited - [Duty of Care Delegations Manual](#)

<b>Date Last Reviewed:</b>	June 2021
<b>Policies folder</b>	Care, Safety and Welfare of Students/ICT Acceptable Use Agreement Policy
<b>Staff Handbook Section</b>	1) Pastoral Care/Mobile Phones and Digital Devices
	2) Policy and Procedures/ICT Policy