



Catholic College Sale

ACCEPTABLE USE OF DIGITAL TECHNOLOGIES POLICY

1.0 POLICY AUTHORITY

The Board of Catholic College Sale Limited ('the Board') governs the College. Based on the principle of subsidiarity and in keeping with the Board's Delegations Schedule, the Board delegates a broad range of duties, functions, powers and authority to the Principal of Catholic College Sale (CC Sale). This includes the effective implementation of this *Acceptable Use of Digital Technologies Policy* and the compliance obligations outlined herein.

2.0 INTRODUCTION

Catholic College Sale recognises the importance of digital technologies in supporting teaching and learning. The College also recognises that education in cyber safety is essential – it not only reduces students' exposure to cyber risks but also develops them as responsible cyber citizens who demonstrate ethical behaviour when using online and digital technologies.

3.0 PURPOSE

This policy presents the College's expectations of students and all members of the community in promoting and supporting the safe and responsible use of digital technologies. It incorporates both College provided devices and the students' personal devices. It applies when students are attending the College and/or participating in approved off-campus excursions and extra-curricular activities.

4.0 PRINCIPLES

- 4.1 Digital technologies support teachers to deliver the curriculum and target teaching to address the needs of all students.
- 4.2 Access to digital technologies supports students to be confident users of digital technologies.
- 4.3 The use of digital technologies requires safe, ethical and respectful communication and collaboration, ensuring every student's safety.
- 4.4 Staff have a duty of care to take reasonable steps to protect students from any harm that should have reasonably been foreseen, including those that may be encountered within off-campus learning environments.
- 4.5 Cyber safety and responsible online behaviour are essential in the lives of students and are best taught in partnership between home and the College.

- 4.6 Students are responsible for their conduct when using the College's network and digital resources. They must comply with the College's expectations and honour the College's *Digital Technologies User Agreement*.
- 4.7 Compliance with accompanying school policies and practices pertaining to child safety and Victoria's Child Safe Standards (in particular Standard 9 under Ministerial Order No. 1359) is essential in supporting a culture of responsible cyber citizenship and online safety for students.
- 4.8 The College's practice in the use of digital technologies is informed by the Australian Government eSafety Commissioner.

5.0 DEFINITIONS

Cyberbullying – when a person is threatened, harassed, humiliated, embarrassed or targeted by another person using the internet, mobile phone, instant messaging, e-mail, chat rooms and social networking sites such as Facebook and Twitter, or any other type of digital technology.

Digital technologies – electronic tools, systems, devices and resources that generate, store or process data.

Digital learning – any type of learning that utilises digital technology.

Applications (Apps) – software programs that run on a computer or mobile device. Web browsers, email programs, games and utilities are all applications.

6.0 USE OF DIGITAL TECHNOLOGIES

6.1 Applications

Students access endorsed applications to support learning, collaboration and information sharing. Student work may be shared between teacher and student, student and student, student and parent, and with permission, within the broader school community. When sharing work, teachers will ensure that students understand and observe protocols and procedures. The work shared, including images, videos and presentations, remain the property of the school and cannot be copied, published or distributed in any other forum without permission.

6.2 Cloud Storage

The College utilises cloud storage solutions (such as Google Drive and Microsoft 365) for the storage of documents and presentations. Cloud storage enables collaboration among staff and students, and provides ready access to information across multiple devices. The Catholic Education Office, Diocese of Sale (CEOSale) ICT services, in partnership with the College, provides managed access to cloud-based applications through the use of usernames and passwords. Considerations when accessing school resources outside of the school environment include:

- the use of secure, safe and reliable internet connections
- safe and appropriate storage of important documents
- a safe internet browser free of viruses and a virus-free device
- the use of secure username and passwords.

6.3 School Email

Students have an assigned school email address. Students have a responsibility to use their school email appropriately and in accordance with the College's expectations of appropriate use of digital technologies. A student's email account is not permitted to be used for online transactions, participating in forums or for accessing third party applications for personal, outside-of-school use.

6.4 Digital Media

Students will be provided with access to endorsed digital media, i.e. online text, audio, video and graphics which support the delivery of curriculum.

6.5 Remote Learning

During Remote schooling periods (e.g. due to COVID-safe regulations), the College will implement a program that ensures continued learning for students. This will be facilitated through the use of a variety of online learning platforms.

Engaging in lessons through an online learning platform will allow students to maintain regular weekly contact with their individual teacher/tutor, supporting their continued development and providing them with some degree of normality towards what would be their normal school day.

7.0 DIGITAL TECHNOLOGIES USER AGREEMENT

7.1 Signed Consent

CC Sale students are issued with a *Digital Technologies User Agreement* which is signed on enrolment and valid until the student exits the College. Students are expected to be familiar and compliant with the expectations, rules and conditions contained in the Agreement. There is also an acknowledgement section for parents and guardians/carers to declare their understanding of and consent with the Agreement.

7.2 Monitoring and Compliance

The College reserves the right to capture, store and review all digital materials used across its platforms and network and to review materials on devices owned by the College. Students should not expect that that any information or document transmitted or stored on the platforms/network is private.

Breaches of this policy and the *Digital Technologies User Agreement* may result in disciplinary action, including a loss of privileges in using the College's technology resources. The disciplinary action taken will be guided by the nature of the breach and CC Sale's *Student Behaviour Management Policy*.

8.0 PROCESSES AND PROCEDURES

8.1 The Principal and College Leadership will:

- Implement and regularly review this *Acceptable Use of Digital Technologies Policy*, the *Digital Technologies User Agreement* for students, and the *Cyber Safety Policy*;
- Ensure a whole school approach to determine the use of ICT;
- Ensure a whole school approach to cyber safety education;
- Respond promptly to any inappropriate use of ICT;
- Regularly communicate this policy to staff and promote the importance of cyber safety;

- Ensure staff, volunteers and contractors understand and uphold the College's *Child Safety Code of Conduct* and *Child Safety and Wellbeing Policy*;
- Provide the community with access to cyber safety information via the Australian Government [eSafetyCommissioner](#).

8.2 School staff are expected to:

- Support this policy and school-based procedures;
- Uphold the College's Child Safety Code of Conduct and expectations pertaining to online conduct;
- Create and maintain safe access to ICT for students;
- Ensure that the use of the College's ICT resources are used exclusively for the implementation of the curriculum and supporting the progression of student learning;
- Address cyber safety in line with the College's *Cyber Safety Policy*
- Manage content access based on Australian classifications and age restrictions. (Refer the [eSafetyCommissioner – eSafety Guide](#));
- Participate in appropriate professional learning and training that supports the care, safety and welfare of students online.
- Manage inappropriate use utilising appropriate policies and procedures, including CC Sale's:
 - *Student Behaviour Management Policy*
 - *Student Behaviour Monitoring and Support Policy*
 - *Digital Technologies User Agreement*
 - *Anti-Bullying and Bullying Prevention Policy*
 - *Cyber Safety Policy*
 - *BYOSD Policy*
 - *Mobile Phone Use Policy*.

8.3 Students are expected to:

- Abide by school policies and procedures;
- Cooperate with staff in ensuring a cyber-safe environment;
- Sign and abide by the *Digital Technologies User Agreement*;
- Contribute positively to the development of safe and inclusive online learning environments;
- Appropriately report incidents of improper use and cyber bullying;
- Maintain device settings to ensure that device access, integrity and security are not compromised;
- Ensure they do not share usernames or passwords.

8.4 Parents and guardians/carers are expected to:

- Sign and support the *Digital Technologies User Agreement*;
- Report incidents of cyber bullying to their child's Pastoral Teacher, House Leader or a Child Safeguarding Officer;
- Work in partnership with the College to ensure the safety of students in the online environment;
- Support their child through the creation of an eSafe home environment.

The College emphasises that while it makes every effort to provide students with a safe and educational online environment, student use of technologies that sit outside of the College network is not controlled, and student behaviour and actions cannot be monitored. Parents and guardians/carers are advised to take the necessary and appropriate steps to ensure that their home internet services are suitably secured, filtered and controlled to safeguard their children.

9.0 EXPECTED OUTCOMES

- 9.1 All members of the College community are familiar and compliant with this policy.
- 9.2 Every student has a signed *Digital Technologies User Agreement*.
- 9.3 College community members work respectfully and collaboratively in support of a cyber safe and child safe online environment.

10.0 REFERENCE

State of Victoria, *Child Safe Standards - Managing the Risk of Child Abuse in Schools and School Boarding Premises*, Ministerial Order No. 1359

11.0 RELATED COLLEGE POLICIES & DOCUMENTS

- Anti-Bullying and Bullying Prevention Policy
- BYOSD Policy
- Child Safety and Wellbeing Policy
- Child Safety Code of Conduct
- Cyber Safety Policy
- Mobile Phone Use Policy
- Digital Technologies User Agreement
- Staff Use of Social Media Policy
- Student Behaviour Management Policy
- Student Behaviour Monitoring and Support Policy

12.0 MONITORING AND REPORTING

The Board is responsible for monitoring the implementation of this policy and for providing reports as required to the members of the company, i.e., the Bishop of Sale and the Provincial of the Marist Brothers Australia Limited (MSA Ltd).

The Principal is responsible for:

- Ensuring compliance with the obligations outlined in this policy;
- Assigning authority, responsibility and accountability at appropriate levels within the College for policy implementation and compliance;
- Providing delegated staff with the direction, support and resources necessary to fulfil policy requirements;
- Ensuring cyclic reviews of the policy and recommending to the Board any revisions that may be required to accommodate changes in legislation and diocesan directives;
- Reporting and escalating concerns, issues and policy breaches to the Board and working collaboratively with the Board to resolve them.

13.0 APPROVAL

Approved by	CC Sale Ltd Board
Person(s) Responsible	Principal
Date(s) Reviewed or Updated	June 2022
Next Review Date	June 2024