Catholic College Sale
CYBER SAFETY 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 *Cyber Safety Policy* and the compliance obligations outlined herein.

2.0 INTRODUCTION

Catholic College Sale is committed to providing a safe and secure learning environment for students. The College recognises the importance of digital technologies as a learning tool and endeavours to reduce students' exposure to cyber risks, whilst also developing students as responsible cyber citizens who demonstrate ethical behaviour when using online and digital technologies.

Cyber safety refers to the safe and responsible use of digital technologies. This includes privacy and information protection, respectful communication, and knowing how to get help to deal with online issues. A whole school approach is used to develop a culture of safety and to prevent risks to online safety.

Cyber safety issues can include, but are not limited to, online grooming, cyber bullying, trolling, scams,image-based abuse, and access to inappropriate content. Compromises to cyber safety can occur on a range of devices such as portable wireless devices, smart phones and watches, tablets and home computers, and can take place in both a school and non-school environment.

3.0 PURPOSE

This policy sets out the way in which cyber safety is enhanced at CC Sale and risks to student safety are addressed. It complements the College's *Acceptable Use of Digital Technologies Policy*.

4.0 PRINCIPLES

4.1 Every student has a right to be safe in both physical and online environments.

4.2 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.

4.3 Learning technologies are expected to be used ethically and responsibly in the school environment.

4.4 A whole school approach is adopted to address cyber safety.

4.5 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 online safety for students.

5.0 DEFINITIONS

Cyber abuse – behaviour that uses technology to threaten, intimidate, harass or humiliatesomeone — with the intent to hurt them socially, psychologically or even physically. Cyber abuse can take place on social media, through online chat and messaging services, text messages, emails, on message boards and in online forums that allow people to comment publicly.

Cyber bullying – the use of technology to bully someone — to deliberately and repeatedly engage in hostile behaviour to hurt them socially, psychologically or even physically. It is generally used to refer to the online abuse of children and young people. Groups and individuals can be both the perpetrators and targets of cyber bullying. Cyber bullying can take place on social media, through online chat and messaging services, text messages, emails, onmessage boards and in online forums that allow people to comment publicly.

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

Inappropriate content – material that is illegal or developmentally inappropriate that is shared or accessed online. This can include posting of inappropriate images or comments. It can also include accessing online platforms that contain explicit harmful material.

Grooming – when an adult deliberately establishes an emotional connection with a child in order to lower their inhibitions, and to make it easier to have sexual contact with them. It may include adults posing as children in chat rooms or on social media sites to 'befriend' a child in order to meet with them in person. Grooming can include obtaining intimate images of youngpeople.

Image-based abuse – when intimate photos or videos are shared online without the consent of the person in the photo or video. Even threatening to share intimate images in this way is image-based abuse. It is a criminal offence under state and territory laws. Alternative terms for image-based abuse include 'non-consensual sharing of intimate images', 'revenge porn' or 'intimate image abuse'. Image-based abuse can also arise when a photo or video is digitally altered (for example, photoshopped), or when a person is depicted without religious or cultural attire which they would usually wear in public.

Scams – dishonest schemes that seek to take advantage of people to gain benefits such as money or access to personal details.

Trolling – when a user intentionally makes inflammatory comments in an online public forum in order to provoke anger or argument and disturb other users. Individuals who engage in trolling (called 'trolls') seek an emotional response from others, whether with malicious or humorous intent. Responding to trolling comments can result in an escalation of inappropriate communication.

6.0 PROCEDURES

6.1 Safe use of digital technologies at CC Sale is guided by the College's *Acceptable Use of Digital Technologies Policy* and by the College's expectations outlined in our *Digital Technologies User Agreement.*

6.2 Safe use of digital technologies is also underpinned by the behaviours described in our Whole School Approach to Positive Behaviour Support School Wide Expectations. At CC Sale, a supportive environment is promoted which encourages the development of positive relationships and communication between staff, students, parents and guardians/carers.

6.3 Students are responsible for their behaviour 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.*

6.4 Reporting of cyber safety incidents is encouraged, taken seriously and promptly addressed. Cyber safety response strategies are tailored to the circumstances of each incident.

6.5 Cyber safety and responsible online behaviour are essential in the lives of students and are best taught in partnership between home and the College. Information is regularly provided to parents/guardians/carers to raise awareness of cyber safety as a community issue.

6.6 Cyber safety education and cyber bullying prevention strategies are implemented across year levels on a continuous basis, with a focus on teaching age-appropriate content, skills and strategies to empower students to recognise cyber safety issues and respond appropriately. Online safety risks addressed include:

- cyberbullying/trolling
- invasion of privacy or digital surveillance
- inappropriate sharing of images
- phishing, harvesting of personal information or data theft
- identity theft
- malevolent software (malware)
- offensive images and messages
- age-inappropriate online content
- impersonation/catfishing
- grooming.

6.7 The College's *Anti Bullying and Bullying Prevention Policy,* incorporating cyber bullying, encourages a culture that is firm about the unacceptable nature of bullying. It articulates how bullying and cyberbullying are defined and addressed, including the means taken to prevent incidents and the response taken when bullying or cyberbullying occurs.

6.8 Responsible bystander behaviour is encouraged amongst students, staff and parents/guardians/carers (this may occur where a bystander observes inappropriate online behaviour either being perpetrated by, or targeted at, a student.

6.9 The College's practice in the use of digital technologies is informed by the Australian Government eSafety Commissioner.

7.0 EXPECTED OUTCOMES

7.1 Students, staff and parents/guardians/carers understand the range of cyber

safety risks that exist online.

7.2 Students know how to keep themselves safe online.

7.3 Students are confident in reporting cyber safety issues.

7.4 Cyber safety concerns and complaints are addressed in a timely matter, with the responses tailored to the circumstances of each incident.

8.0 REFERENCES

Australian Government (2020). eSafety Commissioner. Retrieved from: https://www.esafety.gov.au

Australian Institute of Family Studies (2018).*Online Safety*. Retrieved from: https://aifs.gov.au/cfca/publications/online-safety

Reach Out Australia (2020). Technology and Teenagers. Retrieved from: https://parents.au.reachout.com/skills-to-build/wellbeing/technology-and-teenagers

Department of Education and Training (DET) 2018, *PROTECT: Identifying and responding to all forms of abuse in Victorian schools*

Department of Education and Training (DET) 2018, PROTECT*: Identifying and Responding to Student Sexual Offending*

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

9.0 RELATED COLLEGE POLICIES & DOCUMENTS

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

10.0 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.

11.0 APPROVAL

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