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 (the College). This includes the effective implementation of this *Cyber Safety Policy* and the compliance obligations outlined herein.

2.0 INTRODUCTION

The College is committed to providing a safe and secure learning environment for all its students. The College recognises the importance of digital technologies as a learning tool. It is committed to reducing 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 information and communication technologies. This includes privacy and information protection, respectful communication, and knowing how to seek help when dealing with online issues. A whole school approach is used to develop a culture of safety and prevent risks to online safety.

Cyber safety issues can include, but are not limited to: online grooming, cyberbullying, trolling, scams, image-based abuse, and access to inappropriate content. Evolving risks also include misuse of Artificial Intelligence (AI), such as AI-generated deepfakes, automated scams, or AI chatbots being used to impersonate trusted individuals or fellow students.

Compromises to cyber safety can occur on a range of devices, including school laptops, smartphones, watches, tablets, and home computers, and can take place in both school and non-school environments.

3.0 COMMITMENT TO CHILD SAFETY

The College holds the care, safety and well-being of children and young people as a central and fundamental responsibility of Catholic education. This commitment is drawn from and inherent to the teaching and mission of Jesus Christ, with love, justice and the sanctity of each human person at the heart of the Gospel.

4.0 PURPOSE

This Policy sets out the way in which cyber safety is enhanced and issues are addressed at the College.

5.0 PRINCIPLES

5.1 Every child and young person has a right to be safe.

5.2 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 the online learning environment.

5.3 Learning technologies are used ethically and responsibly in the school environment.

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

6.0 DEFINITIONS

Acceptable Use Policies: are documents created by education systems or schools to outline what is acceptable behaviour when using computer facilities and other technologies such as mobile phones.

Cyber abuse: is behaviour that uses technology to threaten, intimidate, harass or humiliate someone, 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.

Cyberbullying: is the use of technology to bully someone, deliberately and repeatedly engaging 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 cyberbullying. Cyberbullying 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.

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

Grooming: is 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 young people.

Image-based abuse: is 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, photo-shopped), AI-generated, or otherwise manipulated or when a person is depicted without religious or cultural attire that they would usually wear in public.

Scams: are dishonest schemes that seek to take advantage of people to gain benefits such as money or access to personal details. Increasingly, scams may also use AI to create more convincing messages, voices, or images to deceive individuals.

Trolling: is 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. AI tools may also be used to automate trolling or generate harmful content at scale.

7.0 PROCEDURE

7.1 Safe use of ICT at the College is guided by the College's *Acceptable Use of Digital Technologies Policy*.

7.2 Safe use of ICT is underpinned by the behaviours described in our CCS School Wide Expectations Matrix

7.3 Cyber safety response strategies are tailored to the circumstances of each incident.

7.4 Cyber safety and cyber bullying prevention strategies are implemented within the College on a continuous basis, with a focus on teaching age-appropriate content, skills and strategies to empower staff, students and parents, guardians or carers to recognise cyber safety issues and respond appropriately. This includes raising awareness of risks linked to AI, such as manipulated media (deepfakes), automated harassment, or AI-assisted fraud.

7.5 Information is regularly provided to parents, guardians or carers to raise awareness of cyber safety as a College community issue.

7.6 A supportive environment is promoted through the Whole School Approach to Positive Behaviour Support, which encourages the development of positive relationships and communication between staff, students and parents, guardians or carers.

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

7.8 Reporting of cyber safety incidents is encouraged, taken seriously and addressed. (e.g. fake profiles, generated images, or automated scams). Additional technical analysis may be required.

8.0 EXPECTED OUTCOMES

8.1 Students, staff and parents, guardians or carers will understand the range of cyber safety risks that exist online, including risks associated with AI-generated content.

8.2 Students will know how to keep themselves safe online.

8.3 Students will be confident in reporting cyber safety issues.

8.4 Cyber safety issues will be addressed in a timely manner, with the responses tailored to the circumstances of each incident.

9.0 APPROVAL

Approved by	CC Sale Ltd Board
Person(s) Responsible	Principal
Date(s) Reviewed or Updated	September 2025
Next Review Date	September 2027