Diocese of Sale
Catholic Education Ltd

Inspiring Faith Inspiring Learning

CYBER SAFETY POLICY

1.0 INTRODUCTION

DOSCEL schools are committed to providing safe and secure learning environment for all its students. Schools recognise the importance of digital technologies as a learning tool and are 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 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, cyberbullying, trolling, scams, image-based abuse, and access to inappropriate content. Compromises to cyber safety can occur on a range of devices such as school laptops, smart phones and watches, tablets and home computers and can take place in both a school and non-school environment.

2.0 PURPOSE

This policy sets out the way in which cyber safety is enhanced and issues are addressed in DOSCEL schools.

3.0 PRINCIPLES

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

3.2 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.

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

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

4.0 DEFINITIONS

4.1 **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.

4.2 **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.

4.3 **Cyberbullying** is 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 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.

4.4 **Inappropriate content** is 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 material.

4.5 **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.

4.6 **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, photoshopped), or when a person is depicted without religious or cultural attire which they would usually wear in public.

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

4.8 **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.

5.0 PROCEDURES

5.1 Safe use of ICT at school is guided by the school's Acceptable Use Policy.

5.2 Safe use of ICT is underpinned by the behaviours described in our Whole School Approach to Positive Behaviour Support School Wide Expectations.

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

5.4 Cyber safety and cyber bullying prevention strategies are implemented within the school on a continuous basis, with a focus on teaching age-appropriate content, skills and strategies to empower staff, students and parents/carers to recognise cyber safety issues and respond appropriately.

5.5 Information is regularly provided to parents/carers to raise awareness of cyber safety as a school community issue.

5.6 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/carers.

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

5.8 Reporting of cyber safety incidents is encouraged, taken seriously and addressed.

6.0 EXPECTED OUTCOMES

6.1 Students, staff and parents/carers will understand the range of cyber safety risks that exist online.

6.2 Students will know how to keep themselves safe online.

6.3 Students will be confident in reporting cyber safety issues.

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

7.0 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

Diocese of Sale Catholic Education Limited (2020*). Whole School Approach to Positive Behaviour Support: Universals*. Warragul: Diocese of Sale Catholic Education Limited.

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

PROTECT - Identifying and Responding to Student Sexual Offending

PROTECT – Identifying and Responding to All Forms of Abuse in Victorian Schools

FOUR CRITICAL ACTIONS FOR SCHOOLS Responding to Incidents, Disclosures and Suspicions of Child Abuse

8.0 RELATED POLICIES

Acceptable Use of ICT Policy

Behaviour Management Policy

Bullying Prevention and Intervention Policy

Child Protection Policy

Child Safety Code of Conduct

Pastoral Care Policy

9.0 REVIEW

Implementation Date: May 2020

Review Date: May 2022