DIGITAL LEARNING AND ACCEPTABLE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY POLICY

1.0 INTRODUCTION

St Michael's Catholic Primary School, Heyfield (the School) recognises the essential role of digital technologies in supporting high-quality teaching and learning. In line with *Ministerial Order No. 1359 – Implementing the Child Safe Standards*, the School is committed to maintaining a safe and secure digital learning environment that protects students from harm and supports their wellbeing.

Digital technologies are integral learning tools. The School enables students to become confident, responsible and ethical users of digital technologies and Information and Communication Technology (ICT) who engage safely and respectfully in online and digital environments. Increased access to digital technologies provides interactive, collaborative and personalised learning opportunities, helping students create high-quality content and engage in meaningful communication.

Digital learning also supports the development of critical skills and knowledge, preparing students to participate effectively in a globally connected world. Through the promotion and teaching of cyber safety, the School aims to empower students to use digital technologies appropriately, reach their personal best, and contribute positively to their communities.
As required by the Victorian Curriculum F–10, digital technologies form a mandated component of learning. The School supports effective use of these technologies including, for example, the internet, applications (apps), computers, tablets and smart phones, by establishing clear expectations, safe practices and consistent protocols for all users.

2.0 PURPOSE

This Policy affirms the School's commitment to providing students with meaningful opportunities to use digital technologies that enhance learning and development through school approved tools, devices and platforms and describes the expected student behaviour when using digital technologies, including the internet, social media and personal or school owned digital devices.

The Policy promotes the safe, responsible and discerning use of digital technologies, including appropriate responses when risks or concerns arise online, prioritising student safety whenever digital technologies are used for learning.

The Policy supports students to develop confidence, capability and ethical practice in their use of digital technologies, including safe, respectful and appropriate communication and collaboration.

The Policy reinforces staff duty of care by ensuring reasonable steps are taken to protect students from foreseeable harm in digital and online learning environments through a whole school approach to digital learning and ICT use.

This Policy informs the *Digital Learning and Acceptable Use of Information and Communications Technology Procedures*.

3.0 CATHOLIC MISSION

The School brings to life the mission of the Catholic Church by engaging and aligning all efforts toward the achievement of DOSCEL's vision for education: *faith-inspired educational excellence for a hope filled future*.

4.0 COMMITMENT TO CHILD SAFETY

The School holds the care, safety and wellbeing of children and young people as a central and fundamental responsibility of Catholic education. This commitment is drawn from the teaching and mission of Jesus Christ.

5.0 SCOPE

This Policy applies to school staff who use digital technology.

This Policy applies to all students within the School and applies to the use of digital technology both during school hours and when engaged in school-related learning activities at home.

6.0 OUTCOMES

6.1 Digital technology enables effective curriculum delivery and supports personalised learning tailored to individual student needs.

6.2 Students confidently and responsibly use digital technology, demonstrating proficiency across tools and safe navigation of online platforms.

6.3 Safe, ethical and respectful digital communication is practiced school-wide, supported by a strong culture of digital citizenship.

6.4 Students understand key digital concepts, including privacy, intellectual property, password protection and safe online behaviour.

6.5 The School mitigates online risks while upholding each child's right to privacy, information access, social connection and learning opportunities.

6.6 Breaches of acceptable use are managed through staged responses consistent with school behaviour policies.

6.7 Staff uphold their duty of care by monitoring digital learning environments and responding to concerns using established protocols.

6.8 Students are appropriately supervised during all digital learning, including virtual and off-site programs.

6.9 A whole-school approach embeds positive digital behaviour, digital learning and ICT expectations and safe online practices within policies, curriculum and daily routines.

6.10 Filtered internet services are provided, and suspected illegal online activity is referred to relevant authorities.

6.11 Digital learning and ICT practices align with Australian Government eSafety Commissioner guidance, ensuring up-to-date and evidence-based approaches.

6.12 Families are supported to understand safe digital use through regular communication and information sessions.

6.13 Use of school devices and digital technologies requires a signed A*cceptable User Agreement*.

6.14 DOSCEL Office may access and monitor school network communications, where required.

6.15 Students and staff feel physically, emotionally and digitally safe, supported by clear protocols, ongoing training, and timely responses to online concerns.

7.0 DEFINITIONS

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

Applications (Apps): are software programs that run on a computer or mobile device. Web browsers, e-mail programs, word processors, games and utilities are all applications.

Cyber Safe (or e-safety) is the safe, responsible and ethical use of digital technology and ICT. It involves educating students to protect their privacy, manage digital footprints, avoid inappropriate content, prevent cyberbullying, and cultivate positive, respectful online relationships.

8.0 COMMUNICATION

This Policy is available on the school policy portal and provided to parents upon request.

This Policy is available to staff through the staff portal and staff are annually upskilled on this Policy.

9.0 POLICY INFORMATION

Policy Owner	Catholic Identity, Leadership, Learning and Teaching
Approving Authority	DOSCEL Board
Assigned Board Committee	Catholic Identity, Leadership, Learning and Teaching
Board Approval	20 February 2026
Risk Rating	Medium
Implementation	March 2026
Review Date	2028

POLICY DATABASE INFORMATION	
Supporting Documents	Duty of Care Policy Acceptable User Agreement

Appendix 1

Cyber Safety Information Sheet

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—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.

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.

Grooming is when an adult deliberately establishes an emotional connection with a child 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 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), or when a person is depicted without religious or cultural attire which 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.

Trolling is when a user intentionally makes inflammatory comments in an online public forum 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.