Melbourne Archdiocese
Catholic Schools

ICT Acceptable Usage Policy – Students

1. Introduction

Melbourne Archdiocese Catholic Schools Ltd (**MACS**) is a company limited by guarantee established in 2021 by the Archbishop of the Catholic Archdiocese of Melbourne to assume the governance and operation of MACS schools across the Archdiocese of Melbourne. MACS subsequently established Melbourne Archdiocese Catholic Specialist Schools Ltd (**MACSS**) to provide educational services to children with diverse learning needs and Melbourne Archdiocese Catholic Schools Early Years Education (**MACSEYE**) to provide early years care and education services.

The Statement of Mission in the MACS Constitution, and the constitutions of its subsidiaries, MACSS and MACSEYE, sets out the Archbishop's expectations of Catholic schooling in the Archdiocese and provides an important context and grounding for the company and the direction which the MACS Board must always observe in the pursuit of the company's objects.

The Board must ensure that all policies and procedures concerning the operations of MACS, and its subsidiaries are consistent with the Statement of Mission and company objects, as well as any directions issued by the Archbishop from time to time.

2. Background

MACS 2030 highlights that 'Catholic education seeks to provide the young with the best kind of education possible, one that fosters a formation of the whole person that is deeply and enduringly humanising' as such student growth and skill development in the use of digital tools is part of this formation.

By establishing clear statements about the use of information and communication technologies (ICT), this policy supports the effective delivery of education, protects the dignity and wellbeing of the students we seek to educate in digital citizenship and the mitigation of risks associated with online activities, while fostering an environment of trust and integrity.

3. Purpose

The purpose of this policy is to outline the expectations for student behaviour when online and engaging in digital environments.

4. Scope

This policy applies in MACS schools, including specialist schools operated by MACSS and school boarding premises operated by MACS schools (**MACS Schools**). It applies to all students in MACS schools who access or use MACS's ICT. It encompasses all digital devices, networks, online platforms, and related resources provided or approved by MACS or MACS schools, whether accessed on-site or remotely.

In line with the requirements of the Child Safe Standards, MACS schools provide physical and online environments that promote safety and wellbeing while minimising the opportunity for children and young people to be harmed. Principals are responsible for ensuring age-appropriate strategies and practices are in place to assist in protecting students from risks in online environments which aligns with the application of the Victorian Child Safe Standards and all online legislative requirements.

5. Principles

These principles for student use of ICT within MACS schools draw on *MACS 2030* and are aligned with MACS' Vision for Instruction and Vision for Engagement. Students will:

- respect the dignity, privacy, and safety of all individuals, recognising the inherent dignity of every person as being created in the image of God.
- experience a learning environment where ICT is used to enhance their education, support excellence, foster innovation and promote collaboration.
- become informed, responsible, and ethical digital citizens adhering to all legal and policy requirements
- understand about cyber safety and data privacy and how to mitigate the risks involved
- feel confident that technology used as part of their learning reflects Catholic beliefs and ethos to provide the very best Catholic education to all students enrolled in our schools.
- feel safe, empowered, and able to participate in the digital environment.

6. Child safety in online environments

MACS has zero tolerance for child abuse. The use of ICT in MACS schools reflects Catholic beliefs and ethos, as well as the professional expectations and standards for teachers to create supportive and safe learning environments. In keeping students safe online, MACS teachers are also required to adhere to the Code of Conduct for MACS Staff.

MACS acknowledges its duty of care to ensure that all students engage with ICT in a safe, supportive and inclusive environment, consistent with Child Safe Standard 9.

Staff are required to promptly raise concerns regarding inappropriate or unsafe use to the Principal or another relevant member of the school leadership team.

7. Internet and network access

Students are provided access to the internet and school networks to support educational and administrative activities. Network permissions consider and adhere to legislative requirements.

In line with the Student Bullying Prevention and Response Policy, Principals and school leadership teams must implement school-wide, age and culturally appropriate approaches and measures to educate and inform the school community about bullying including cyberbullying, and its prevention, and an approach to the safe and respectful use of ICT.

Principals will maintain a list of digital applications and tools used in the school and provide this information to Parents when requested. The Privacy Policy and Privacy Collection Notice – Students and Parents provides further guidance to Principals.

The expectations for student behaviour will always reflect the values of the school and those outlined in the Student Code of Conduct and other MACS and school policies and processes.

8. Safe ICT use and responsibilities

MACS is committed to protecting students and keeping them safe online. There are a range of actions that MACS undertakes to mitigate privacy and child safety risks to ensure student safety when using MACS, or school provided digital systems, devices and tools. These include:

- the provision of digital systems, devices and tools by MACS/Schools to adhere to all relevant legislative requirements, including, but not limited to: Child Safety – Ministerial Order 1359 and Child Safe Standards, *Online Safety Act 2021*, *Online Safety Amendment (Social Media Minimum Age) Act 2024*, *Copyright Act 1968,* and the Australian Privacy Principles (APP).
- safeguards in the Cyber Security Policy and Standards, which are benchmarked against the NIST Cybersecurity Framework.
- application of safeguards including filtered internet access and digital monitoring, whilst fostering a culture of respect and transparency.

- establishing cultural safety and the sharing of the responsibility to protect and educate students in the development of moral and ethical digital citizenship through curriculum and / or student wellbeing programs.
- working in partnerships with families to support the implementation of these

safeguards. Principals in MACS schools will:

- expect teachers to supervise and support students when using ICT as part of their learning.
- take reasonable steps to select digital tools that are safe by design and secure for student learning.
- provide additional protection for vulnerable students or students with additional needs for their use of ICT.
- obtain parent consent for any digital tools where uploaded content is visible to the public.
- ensure all use of ICT has an appropriate educational purpose and is consistent with MACS expectations.
- regularly review and document the digital tools used in school.

9. Expectations for Students

Teachers will use age-appropriate language and strategies to explain this policy to students (see Acceptable Use Agreement – Students, F–4, 5–8 and 9–12).

9.1. Safe and responsible online student behaviours

Acceptable online behaviours are outlined in the related procedures listed below:

- Acceptable Use of ICT Agreement for Students – Years F– 4
- Acceptable Use of ICT Agreement for Students – Years 5 – 8
- Acceptable Use of ICT Agreement for Students – Years 9 –12

These Agreements detail expectations for respectful online conduct, privacy protection, responsible use of digital tools, and awareness of legal obligations in age-appropriate language for students.

10. What Parents/Carers do to help keep students safe online

MACS schools work in partnerships with families to provide safe online environments for students that protect the dignity and wellbeing of all persons. In this partnership, Parents/Carers are expected to:

- discuss the content of the Acceptable Use of ICT Agreement with their child or young person to help them understand how to remain safe online while reminding them to adhere to the Student Code of Conduct
- adhere to the school's Parent/Carer Code of Conduct and Acceptable ICT User Agreement

11. Monitoring and compliance

Principals in MACS schools reserve the right to monitor all ICT use, including internet activity, email communications, and digital content accessed or created using student devices (BYOD, mandated, or school provided) or school networks. This ensures compliance with the policy, supports the safety and wellbeing of students, and protects the integrity of ICT resources.

Monitoring is conducted in accordance with relevant legal and ethical standards and may include reviewing user activity logs, filtering inappropriate content, and auditing device use (see Steps to Review a Student Device Checklist). Students and parents will be informed that all ICT activity is subject to monitoring to promote a secure and responsible digital environment.

11.1. Breaches of this policy

Breaches of this policy will be address through the following procedures:

- Steps to Review a Student Device Checklist
- Checklist for Suspected ICT breaches – Students

12. Roles and reporting responsibilities

Role	Responsibility	Reporting requirement
Principal	Enact the policy with the school community	Ensure the school community is informed when this policy is reviewed and updated
Principal	Act on and respond to breaches of the policy	Where necessary, escalate breaches to MACS privacy officer or general manager (region)
Principal	Ensure all policies for the care, safety and welfare of students are publicly available and the school community is informed when the policies are reviewed and updated.	Annual attestation as part of the Annual Report to School Community

13. Definitions

Definitions of standard terms used in this Policy can be found in the Glossary of Terms.

Digital citizenship

Skills and knowledge an individual needs to practice ethical, safe, respectful behaviours and responsible participation in online and digital environments.

Digital devices/technologies

Any electronic tool, like laptops, tablets, or phones, that can be used to access, create, or share digital content, this can also include smart watches.

Digital systems

Interconnected hardware, software, and networks that collaboratively process, store, and exchange digital information.

Digital tools

Software or online platforms used for learning, creating, communicating, or managing information digitally (including but not limited to MS 365 CoPilot, Google Workspace for Education Plus) as well as any school purchased tools used in teaching the knowledge and skills necessary to achieve student learning.

Email

The system that enables students to send data over the internet using computers and mobile devices.

Filtering

Restricting access to certain online content or websites based on rules set for safety or appropriateness.

Google Workspace for Education

A suite of cloud-based tools provided by Google, designed specifically for educational institutions. It includes applications like Gmail, Calendar, Drive, Docs, Sheets, Slides, Classroom, and Meet to support communication, collaboration, and learning.

ICT

Information and Communication Technology (ICT) encompasses digital tools, devices, networks, and platforms used for communication, learning, and information management.

Internet

The system of interconnected networks that connects computers for data transmission and storage.

Intranet

A local system of computers enabling students and staff to communicate and share information within their school community.

Mobile devices

Refers to (but is not limited to) mobile phones, smart watches, tablets, and portable storage devices.

Network (services)

The facilities and resources located on and delivered via a computer-based network, including communication systems, internet and intranet services, mobile devices, electronic mail, web services, printer services, database services, back-up services, file services and network management services.

MS 365 CoPilot (formerly Microsoft Office 365)

A cloud-based subscription service offered by Microsoft that provides access to a suite of productivity tools. This includes applications like Word, Excel, PowerPoint, Outlook, Teams, and OneDrive, designed to support communication, collaboration, and productivity.

Parent

A person who has parental responsibility for a child. This may include a biological parent or another person who has been granted parental responsibility by a court order.

Passphrase

A longer password made of multiple words or phrases, used for stronger security and easier recall.

Smart device

An internet-connected device that can perform tasks, collect data, and interact with users through built-in sensors, software, or voice control.

Student

Student means a person who is enrolled at or attends a MACS school.

Website

An internet-based page or series of pages grouped together and managed by a person or group.

14. Related Policies and documents

Supporting documents

Acceptable Use Agreement – Students F – 4
Acceptable Use Agreement – Students 5 – 8
Acceptable Use Agreement – Students 9 – 12
Digital tools – Template for Schools
Steps to Review a Student Device Checklist
Checklist for Suspected ICT breaches – Students

Related MACS policies and documents

Student Bullying Prevention and Response Policy
Child Safety and Wellbeing Policy
Parent / Carer Code of Conduct

Student Code of Conduct
Code of Conduct for MACS Staff
Cybersecurity Policy
Data Policy
Pastoral Care Policy
Privacy Collection Notice – Students and Parents
Privacy Policy
Student Behaviour Support Policy

Resources

Australia eSafety Commissioner Guide
Australian Cyber Security Centre Guidelines
Child Safe Standards
MACS eSafe Behaviours
Making it Real, The Australian Catholic Bishops Social Justice Statement for 2019-2020

15. Legislation and Standards

Privacy Act 1988 (Cth)
Copyright Act 1968 (Cth)
Online Safety Act 2021 (Cth)
Online Safety Amendment (Social Media Minimum Age) Act 2024
Education and Training Reform Act 2006 (Vic)
Education and Training Reform Regulations 2017 (Vic)
Equal Opportunity Act 2010 (Vic)
Privacy and Data Protection Act 2014 (Vic)
Ministerial Order 1359 – Child Safe Standards

Policy information

Responsible executive	Director, Education Excellence
Policy owner	Chief of Education, Strategy and Performance
Approving authority	MACS Executive Director
Assigned board committee	Education Strategy and Policy
Approval date	29 October 2025
Risk rating	High
Review by	October 2026
Publication	CEVN, school website

POLICY DATABASE INFORMATION	
Assigned framework	Care, Safety and Welfare of Students
Supporting documents	See list of supporting documents and related policies above
Superseded documents	ICT Acceptable Use Policy – v1.0 – 2022