

# St Monica's College Epping ICT Acceptable Usage Policy



## Purpose

*'The digital world is characteristic of the contemporary world...the web and social networks have created a new way to communicate and bond...Yet to understand this phenomenon as a whole, we need to realise that, like every human reality, it has its share of limitations and deficiencies.'*  
Pope Francis, *Christus vivit*, 2019.

Access to digital technologies, including the internet, is provided to students and staff at St Monica's College because digital information and communication are important mediums for contemporary learning and teaching and administration. Within Melbourne Archdiocese Catholic Schools (MACS), a range of technology platforms, such as the Integrated Catholic Online Network (ICON) provide access to a suite of digital technologies. The information, communication and learning technologies used by students in classrooms will be appropriate to the age and development of students. These technologies are used to support professional learning and the development of networks within and between St Monica's College and other schools for professional learning. They also enable effective communication with our parents and allow them to participate in their children's education, working in partnership with teachers.

In using and managing internet and network services, students and staff at St Monica's College are expected to respect the rights and privacy of all persons. They are called upon to respect the dignity of every human person. St Monica's College, along with parents in our community, educate students in the use of information and communication technologies to assist them to become responsible users, creators and publishers in the digital environment.

The ICT Acceptable Usage Policy provides guidance for all staff, students and users of the College's information technology resources. The purpose of this policy is to ensure:

- The acceptable and appropriate use of the College Email and Internet systems;
- The acceptable and appropriate use of the College Collaboration and Learning Management systems;
- The acceptable and appropriate use of the College Administration systems;
- Adherence to procedures for core IT processes;
- The provision of reliable and uninterrupted Information Technology services;
- The integrity and validity of data;
- The protection of all College information technology assets including data, software and hardware.

This policy outlines the appropriate use and management of digital technologies such as the internet and network services at St Monica's College in accordance with legal and moral requirements and expectations.

Digital technologies and their use in classrooms are opening up new opportunities for learning, and previously unimagined approaches to teaching and learning.

Today, young people have access to knowledge, people and new ideas like never before. They are able to connect, collaborate and build relationships with peers, educators and the wider global community. The use of digital technologies within Catholic schools supports learners to question,

evaluate and consider the validity of information and then search for truths contained in those ideas. Learners are empowered to demonstrate adaptability and versatility in thinking and strategies as they select, use and manage a range of applications and technologies. We seek to develop students who are responsible and ethical communicators, creators and publishers in the digital community.

## Scope

This policy applies to members of the St Monica's College community including employees, students, contractors, and sessional staff in their use of digital technologies. It applies to all computers, devices, internet and network services, information and communication technologies, applications, and systems provided, operated and managed by the school.

This policy does not apply to the curriculum content or the expected standards of usage by students or staff in the school. The curriculum and teaching practices and pedagogy are outlined in documents related to our learning and teaching programs.

This document describes the access methods, services available, and the user and management responsibilities when using the Network, Internet, Electronic Mail (email), corporate and collaboration facilities within the College. Users who have access to the network have an obligation to use their access in a responsible and informed way. Managers and supervisors have a responsibility to ensure the network and internet is used appropriately within the College.

All College policies, procedures and requirements with regard to ethical & appropriate behaviour, fraud, risk management and records management apply to the use of the Network, Internet, Electronic Mail and Collaboration systems.

## Definitions

**Computer** is either a desktop or portable laptop device that performs processes, calculations and operations based on instructions provided by a software or hardware program.

**Device** refers to a unit of physical hardware or equipment that provides one or more computing functions within a computer system. It can provide input to the computer, accept output or both. Typical hardware includes a computer mouse, speakers, printer and microphone.

**Email** means the system that enables users to send data over the internet using computers and mobile devices.

**ICON** means the Integrated Catholic Online Network which is used to deliver shared services for educational and administrative purposes across Catholic schools.

**Internet** means the system of interconnected networks that connects computers for data transmission and storage.

**Intranet** refers to 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, PDAs and portable storage devices.

**Network services** means 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.

**Parents** includes parents, guardians and carers.

**Social networking** means web-based services that allow individuals to create their own online profiles and communicate with each other by voice, chat, instant message, image sharing, video conference and blogs in a virtual community.

**Staff** means salaried, voluntary and contracted persons.

**Students** means those students enrolled at St Monica's College

**Website** is an internet-based page or series of pages grouped together and managed by a person or group.

## Principles

The use of digital technologies within our school by staff and students at St Monica's College is underpinned by the following principles and understanding:

- that digital technologies provide valuable opportunities for staff and students to collaborate, connect and create with peers, colleagues, experts and the wider community
- that online behaviour will at all times demonstrate respect for the dignity of each person in the community
- users will behave in a manner that is ethical when using the internet and network services (even for personal communication)
- the Catholic beliefs and ethos of the school, and professional expectations and standards required by teachers are demonstrated in the way the technologies are used
- inappropriate online behaviour, including cyberbullying, will not be tolerated.

## Policy

### Internet and Network Access

Access to internet and network services are provided by MACS to staff and students of St Monica's College for educational and administrative purposes. From time to time, other MACS policies and requirements in particular schools may result in restrictions.

Access rights assigned to students and staff at St Monica's College will be determined by the Principal and may vary as educational and administrative purposes change.

Students and staff at St Monica's College may not use the internet and network services provided for commercial purposes, either offering or acquiring goods or services for personal use. The services cannot be used for political lobbying or proliferation of unnecessary communications.

### Electronic Mail (Email) and Collaboration Systems

Corresponding via email and collaboration systems is common across the organisation. It is important to remember that the use of email and collaboration systems should, wherever possible, be restricted to business use. Offensive material should not be instigated by College users and should be deleted immediately. Further, such material should not be forwarded to any internal or external correspondents.

### When sending email or chats

- Regardless of the recipient, act in a professional and courteous manner. Be discreet in what you send. Avoid gossip and personal comments. Avoid sarcasm or irony.
- Once an email or chat has been sent, the sender loses control of what happens to that email or chat, for example whether it is on-sent or who will have future access to view it. Staff

and students must therefore assume that emails or chats sent are not private and may be freely available in the public domain.

- Where possible, use the 'To' field to indicate 'for action' and 'Cc' to indicate 'for information'.
- Use mixed case in email messages. DO NOT use uppercase only.
- Always proof read and spell check messages before sending them.
- Keep your email and chat messages brief and to the point. DO NOT clutter other people's email and chat accounts with unnecessary messages.
- Never forward offensive material to others within or external to the organisation, this includes jokes and video clips. If you receive offensive material, delete it immediately and reply to the sender asking to refrain from sending inappropriate material
- Avoid using coloured or graphical backgrounds, large graphics or illegible fonts.
- Use hyperlinks or cloud storage to include large documents rather than attaching them as files. This will reduce duplication on the email server.
- Immediacy of transmission does not always translate into immediacy of receipt. Where a response is required immediately or the matter is urgent, it might be advisable to consider using other means of communication.

### **Good Housekeeping Practices**

- Check email regularly. Respond to messages promptly. Give a brief acknowledgment if a full response cannot be provided initially.
- Delete unwanted messages immediately and regularly empty the Deleted Items folder.
- Keep messages remaining in electronic mailboxes to a minimum.

### **Ownership and Storage**

Authorised users are responsible for information or information systems accessed via their network account and therefore it is important to maintain security of your network account password. Passwords should never be shared. Further information on security can be found in the IT Security Policy.

It should be noted that all electronic files, emails, data, and accounts on the College's IT systems should be presumed to be the property of St Monica's College.

All incoming and outgoing email messages and chat sessions can be monitored by the IT department and information (including content and contact details) may be kept on file.

Electronic mail and chat sessions may be subject to Freedom of Information and Privacy rules and therefore, individual employees are responsible for anything they write. Email has the same legal status as traditional written correspondence, so employees must apply the same business rules and protocols for email correspondence.

### **Distribution Lists**

The use of the College-wide distribution lists are only for use when the email is College related, important and relevant to the majority of the group being sent to. They are not to be used for soliciting, campaigning or engaging in fund-raising for any organisation, person, charity or other body without the prior permission of the Deputy Principal (Operations).

### **Email Protocol**

Established procedures regarding the signing of official correspondence also apply to email.

All care should be taken to ensure that external email messages are addressed correctly. Messages should also identify where they contain personal opinions.

Employees should not knowingly delete any correspondence that could, at some time in the future, be used as evidence in any potential legal proceedings.

It should be noted that the email system is a communication tool provided by the College to carry out school business (not personal business). Professional ethics require that personal messages be kept to a minimum.

The College permits occasional, reasonable personal use, but this shall not be excessive, and all communications shall comply fully with this policy.

In addition, a degree of caution should also be exercised when sending files within email messages, to ensure that confidential or unrelated files are not inadvertently sent.

### **Generic Email Addresses**

The College corporate email address is [admin@stmonicas-epping.com](mailto:admin@stmonicas-epping.com); emails to this address will be received by the Executive Assistant to the Principal who will distribute the email to the appropriate staff member.

Other mailboxes have been set up for specific purposes and the departments controlling these are responsible for the monitoring and processing of any email received as well as maintaining them in line with good housekeeping practices outlined above.

Generic Email addresses are not to be used unless there is a valid business reason and must be approved by the Director of Information Technology.

### **Downloading files**

The following rules apply to the downloading of files from external sources, including electronic mail and the Internet.

- No games, movies or TV shows will be downloaded onto, or accessed from the Internet from any College device and must not be saved on College file servers unless for educational purposes.
- Pornographic or other material of an offensive nature is NOT to be searched for, downloaded or uploaded. This restriction includes but is not limited to such material in text, graphic, audio or video format. Users are advised that the downloading of pornographic material from the Internet and / or distribution via electronic means may be a criminal offence
- In some instances, offensive or inappropriate material may be inadvertently displayed when searching the Internet via advertising “pop-up” windows etc. Should any such “unsolicited” material be encountered, employees are advised to log out of the sites immediately and warn any other employees who may be affected.
- Employees are advised that content checking software may quarantine such material and bring it to the attention of the Information Technology department.
- Employees are reminded of international copyright and piracy laws and are strictly forbidden to copy any material onto College systems that may breach these laws.
- No computer programs or executable files are to be downloaded onto or installed on any College computer without the written permission of the Information Technology department.

### **Subscriptions to Web Sites**

Some web sites offer information and services to visitors in the form of subscriptions. Most often, subscriptions are free, but visitors are required to provide identification details to access these areas (usually name, company, position and email address).

Subscriptions should be for work purposes only. If there is a need to subscribe to a web site for personal reasons it is recommended that the staff member use a personal email address.

### **Scanning, Filtering and Blocking**

Internet, emails, browsing, chat sessions and downloads are subject to scanning, filtering and blocking processes conducted by automatic content filtering software. These processes aim to conserve College resources and prevent obscene, illegal or inappropriate activity.

College filtering processes may automatically block websites that present a risk to the College and/or are in breach of College policy. Information Technology staff can also manually block problematic sites.

### **Quarantined Messages**

Employees will be notified of any quarantined Email messages or Internet activity. Access to quarantined messages can be obtained by contacting the Information Technology department who may release them if deemed safe and appropriate to do so.

### **Viruses, Scams and Phishing**

Email messages from unknown senders arrive from time to time – sometimes with file attachments and links. Exercise caution before opening attachments or clicking on links. If in any doubt, check with the IT Department or just delete the item.

Be aware too of ‘Phishing’ scams that purport in many cases to be from banks or utility companies may seek usernames, passwords and other personally identifiable information. Regardless of the College’s virus protection measures, it is always possible that newer virus strains may be able to penetrate virus scanning.

### **Expectations of users**

All students and staff at St Monica’s College are required to use the internet and network services in accordance with this policy. Any use of devices or services that may be questionable, offensive, and controversial or against the Catholic ethos is unacceptable. This includes personal communication with students on matters not related to curriculum or education. These standards apply whenever St Monica’s College equipment or communication lines are used, including use from home or other non-school location and when a private account is used.

All students and staff should remember that body language, facial expressions and vocal inflections DO NOT travel with electronic mail or chat messages and be aware in composing messages, that their contents have the potential to be misconstrued by the recipient.

### **Non-compliance with this policy**

Disciplinary action may be undertaken by St Monica’s College against any student or staff member is who found to be inappropriately using the provided internet, network services, device or mobile device.

The principal will determine the disciplinary measures to be undertaken in accordance with other policies and guidelines. These measures may be outlined in staff handbooks or the Acceptable User Agreement for students used by St Monica’s College.

## **Duty of Care**

St Monica's College will provide instruction to students in online personal safety issues, including inappropriate sites, stranger danger, cyberbullying and scams. St Monica's College and our Cyber Safety presenters will prepare staff to deal with these issues.

## **Monitoring**

### **Students**

Online activities may be monitored or reviewed to assess network efficiency, examine system security and to investigate alleged breaches of this policy.

### **Staff**

An authorised person (e.g. a principal, a regional manager or other MACS staff member can monitor the use of MACS ICT resources. Server logs may also be used in an investigation of an alleged breach of this policy.

### **Security**

To minimise risk to MACS information and communication networks from viruses and intrusions, current virus screening software is to be activated, and where appropriate, passwords are to be used by staff and students of St Monica's College. Firewalls are to be maintained. The management of system protocols and configurations are the responsibility of the staff authorised by the school or MACS. Non-authorised staff and students are not permitted to have access to these levels of system management.

### **Email**

Email service is provided for educational and administrative purposes. Staff and students at St Monica's College must identify themselves appropriately by using a signature block at the bottom of the email message that includes their name, school phone number and postal address. St Monica's College advises students and staff that they may be held accountable for the email they create and distribute using the network.

### **Websites**

St Monica's College may create, or have created, a website with the approval of the principal. These websites must be established and maintained in accordance with MACS policies and guidelines and relevant legislation.

### **Social networking**

Provision of social networking for students must be related to an educational purpose. This is at the discretion of the principal.

### **Acceptable Use Agreements**

This policy outlines the expected conduct for staff members and students at St Monica's College when using digital technology.

Students and parents are required to declare their understanding of the Acceptable Usage Agreement.

### **Students**

A copy of the St Monica's College IT Acceptable Use Agreement and this policy can be found on the College Website.

## Staff

Staff are required to use the internet and network services in accordance with this and other policies. St Monica's College provides staff with the following:

- a copy of this policy
- a copy of the Acceptable User Agreement.

## Related school policies

- Anti-Bullying Policy
- Child safety policies
- Codes of conduct for students, parents and staff
- Data Breach Policy
- Managing Complaints and Grievances Policy
- Privacy Policy
- Social Media Policy for staff
- Student Behaviour Policy.

## Appendix 1

### Acceptable User Agreement Declaration

*\*This declaration is signed via a Memorandum of Understanding with Parent and Students. Each time a staff member logs on they agree to the declaration.*

This network is the property of St Monica's College, Epping and is for authorized users only. The use of this network is monitored. Access to this network is subject to your compliance with the St Monica's College ICT Acceptable Usage Policy. Unauthorised or improper use of this network may result in disciplinary action, including termination or expulsion. In logging on to this network I agree to abide by the policy.

I confirm that I have read and understood the ICT Acceptable Usage Policy and I will abide by the rules and regulations within it.

<b>Responsible director</b>	Director, Learning and Regional Services
<b>Policy owner</b>	General Manager, Student and Learning Technologies
<b>Approving authority</b>	MACS Executive Director
<b>Assigned board committee</b>	Education Policy and Strategy
<b>Risk rating</b>	High
<b>Approval date</b>	14 September 2022
<b>Date of next review</b>	April 2023

POLICY DATABASE INFORMATION	
<b>Assigned framework</b>	Care, Safety and Welfare of Students
<b>Related documents</b>	ICT Acceptable User Agreement – Staff ICT Acceptable User Agreement – Students
<b>Superseded documents</b>	ICT Acceptable Use Policy – v1.0 – 2021
<b>New policy</b>	