



## 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. Joseph's School because digital information and communication are important mediums for contemporary learning and teaching and administration. Within 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. Joseph's School 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 netw services, students and staff at St. Joseph's School are expected to respect the rights and privacy of all persons. They are called upon to respect the dignity of every human person. St. Joseph's School, 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.

### Digital Technology use in Classrooms

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.

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

## Scope

This policy applies to members of the St. Joseph's School community 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.

## Rationale

At St Joseph's School, we believe in preparing students for their future by teaching them relevant skills for the environment they live in. To cater for the development of children's needs in an Information Communication Technologies (**ICT**) focused society, we provide facilities and programs that expose children to the ICT of the day and encourage learning through the use of those technologies.

The School provides students with access to the School's Local Area Network (**LAN**) for electronic file storage and collaboration, the Internet, Electronic Mail (**Email**) and ICT hardware including iPads and computers. The educational value of these resources is constantly being evaluated and updated.

Throughout the School, there are physical and wireless connections to the LAN and the Internet. The School makes every effort to ensure that all users are protected from any misuse or abuse as a result of their experiences using the School's ICT facilities but cannot guarantee it.

Access to the LAN and Internet may be monitored by School Staff and it is expected that any use will be for educational purposes only.

## 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 communication 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. Joseph's School.

**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. Joseph's School 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. Joseph's School 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. Joseph's School will be determined by the principal and may vary as educational and administrative purposes change.

Students and staff at St. Joseph's School 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.

### Expectations of users

All students and staff at St. Joseph's School 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. Joseph's School equipment or communication lines are used, including use from home or other non-school location and when a private account is used.

### Non-compliance with this policy

Disciplinary action may be undertaken by St. Joseph's School against any student or staff member 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. Joseph's School.

### Duty of Care

St Joseph's School recognises the need for students to be safe and responsible users of digital technologies. We believe that explicitly teaching students about safe and responsible online behaviours is essential and is best taught in partnership with parents/guardians and teachers. We request that parents/guardians work with us and encourage this behaviour at home.

St. Joseph's School will provide instruction to students in online personal safety issues, including inappropriate sites, stranger danger, cyberbullying and scams. St. Joseph's School 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. principal, Regional General 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 activated, and where appropriate, passwords are used by staff and students of St. Joseph's School. Firewalls will 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. Joseph's School 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. Joseph's School advises students and staff that they may be held accountable for the email they create and distribute using the network.

### Websites

St. Joseph's School 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

The use of ICT, whilst within the grounds of the School, must be in support of education and research and be consistent with educational objectives;

Use of other organisation's networks or computing resources must comply with the rules appropriate for that network;

Uploading or Downloading of any material in violation of any Australian law is prohibited. This includes but is not limited to:

- Copyrighted material
- Threatening or obscene material

Undesirable or inappropriate material is not to be used or downloaded.

## **Privileges**

The use of the School's ICT is a privilege, not a right, and inappropriate use may result in the withdrawal of this privilege and a renegotiation of the user's privileges.

Before gaining access to School ICT, each user and their parent or guardian will be required to read and sign an ICT user agreement. All users and their parent or guardian will then undergo training in the proper use of ICT and associated services.

The Principal may request the ICT Leader to deny, revoke or suspend specific user access.

## **ICT Etiquette**

Users must abide by the generally accepted rules of network and ICT etiquette. These include but are not limited to:

- Not revealing personal information (including addresses, email addresses or telephone numbers) to anyone else;
- Not using inappropriate language;
- Not writing or sending abusive message to others;
- Not using ICT in such a way as to disrupt the use of ICT resources by other users, such as downloading very large files, sending email messages to multiple addresses or usage that annoys other users;

Note: While it is not the intent to read private correspondence, email is not guaranteed to be private. The ICT Leader has access to all mail. Messages relating to or in support of illegal, offensive or bullying activities may be reported to authorities or dealt with by Staff.

## **Privacy**

Please refer to the School's Privacy Policy for information (school website/about us/policy).

## **Security**

Security on School ICT is a high priority as the system serves many users equally. To ensure security of all users, the following practices must be followed:

- Users who identify a security problem must notify Staff or the ICT Leader as soon as possible. They must not demonstrate or highlight the security issue to other users;
- A user who has a password must not disclose it to any other individual;
- Users may only access their own School ICT account;
- Attempts to log into the system by impersonation (using another user's log on details) will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems will be denied access to the School's ICT resources.

## **Damage to or loss of ICT equipment**

Vandalism will result in cancellation of a user's privileges. Vandalism is defined as any malicious attempt to harm or destroy:

- Data found on the School network;
- Computer software;
- Hardware;
- By knowingly spreading computer viruses or malicious software.

*If the school inherit any cost associated to damages or loss, then the person(s) responsible for the damages/loss will inherit the cost.*

## Mobile Phones

### Prep – Yr 4

- Mobile phones are not permitted at school for students in Prep – Yr. 4

### Yr 5 & Yr 6

Students in Yr. 5 & Yr. 6 are allowed to bring a mobile phone, however it is not to be used or carried whilst they are on school property. To facilitate this, all students must:

- Turn off their phone and provide it to their class teacher at the beginning of the school day
- Reclaim their phone from their class teacher prior to departing for the school day

Failure to follow this direction will result in the confiscation of the phone by Staff and a notification to the parent or guardian of the breach of this policy.

## Other Mobile Network Devices

Other devices capable of connecting to the mobile phone network (e.g. smart watches that connect to the mobile phone network) are not permitted at school. Failure to follow this direction will result in the confiscation of the device by Staff and a notification to the parent or guardian of the breach of this policy.

## Acceptance of this Policy

### Students

St. Joseph's School provides students and parents/guardians/carers with the following:

- a copy of St. Joseph's School Acceptable Use Agreement
- a copy of this policy.

The Acceptable Use Agreement is provided in full for consideration by all signatories. The Agreement is to be signed by the student (Yr 3 upwards) and a parent/guardian/carer before the student is given access to, and use of, a school's internet, network services and devices.

### Staff

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

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

## Related school policies

- Anti-Bullying Policy (including cyberbullying)
- Child safety and wellbeing policies
- Codes of conduct for students, parents and staff
- [school name] Complaints Handling Policy
- Privacy Policy
- Social Media Policy: MACS employees
- Student Behaviour Policy
-

<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

<b>POLICY DATABASE INFORMATION</b>	
<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>	



## Student Information Communication Technologies (ICT) Acceptable Usage Agreement

**Parents and guardians play a critical role in developing knowledge, understanding and ethics around their child's safety and safe practices regardless of the time of day. Being cyber-safe is no exception and we invite you to discuss with your child the following strategies to help them stay safe when using ICT at school and after formal school hours.**

1. When at school I will use the computers and other ICT equipment only for my learning.
2. I will go online or use the Internet at school only when a teacher gives permission and an adult is present.
3. If I am unsure whether I am allowed to do something involving ICT, I will ask the teacher first.
4. If I have my own user name, I will log on only with that user name. I will not allow anyone else to use my name.
5. I will keep my password private.
6. I will use the Internet, email, mobile phones or any ICT equipment only for positive purposes, not to be mean, rude or offensive, or to bully, harass, or in any way harm anyone else, or the School itself, even if it is meant as a joke.
7. While at school, I will:
  - a. Only attempt to search for things online that I know are acceptable at our school. This would exclude anything that is rude or violent or uses unacceptable language such as swearing;
  - b. report to a teacher any attempt by other students to get around, or bypass, security, monitoring and filtering that is in place at our school.
8. If I find anything that upsets me, is mean or rude, or that I know is not acceptable at our school, I will:
  - a. not show others;
  - b. turn off the screen; and
  - c. get a teacher straight away.
9. I will not bring other ICT equipment/devices (e.g. mobile phones, iPads, games and cameras) to school.
  - a. If I am in Yr. 5 or Yr. 6 I am permitted to bring a mobile phone to school but must:
    - i. Turn off the phone and provide it to my teacher at the beginning of the school day
    - ii. Reclaim the phone from the class teacher prior to departing for the school dayFailure to follow this direction will result in the confiscation of the phone by Staff and a notification to the parent or guardian of the breach of this policy.
10. Only with written permission from the teacher will I connect any portable ICT device (e.g. USB flash drive) to the school. This includes all wireless/Bluetooth technologies.
11. The school cyber-safety strategies apply to any ICT brought to school.
12. To ensure my compliance with copyright laws, I will download or copy any files such as music, videos, games or programs only with the permission of a teacher or the owner of the original material.



13. I will ask my teacher's permission before I put any personal information online. Personal identifying information includes any of the following:
  - a. my full name;
  - b. my email address;
  - c. photos of me and/or people close to me.
14. I will respect all school ICT and will treat all ICT equipment/devices with care. This includes:
  - a. not intentionally disrupting the smooth running of any school ICT systems;
  - b. not attempting to hack or gain unauthorised access to any system;
  - c. following all school cyber-safety strategies, and not joining in if other students choose to be irresponsible with ICT;
  - d. reporting any breakages/damage to a Staff member.
15. If I do not follow cyber-safety practices the School may inform my parents/guardians. In serious cases, the school may take disciplinary action against me. My family may be charged for repair costs. If illegal material or activities are involved or e-crime suspected, it may be necessary for the school to inform the police and hold securely personal items for potential examination by police. Such actions may occur even if the incident occurs off-site and/or out of school hours.

**PLEASE KEEP THIS PART FOR YOUR REFERENCE**

**To the parent/guardian:**

**Please read this carefully to check that you understand your responsibilities under this Agreement. Return the signed Agreement to the School and keep the second copy for your reference.**

**I understand that the School will:**

- do its best to enhance learning through the safe use of ICT. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or on ICT equipment/devices at school or at school related activities
- work with children and their families to encourage and develop an understanding of the importance of cyber-safety through education designed to complement and support the ICT Acceptable Usage Agreement initiative. This includes providing children with strategies to keep themselves safe in a connected online world
- respond to any breaches in an appropriate manner
- welcome enquiries at any time from parents/guardians or students about cyber-safety issues.

**My responsibilities include:**

- discussing the information about cyber-safety with my child, explaining why it is important
- supporting the school's cyber-safety program by emphasising to my child the need to follow the cyber-safety strategies
- contacting the Principal or nominee to discuss any questions I may have about cyber-safety and/or this Agreement

**PLEASE RETURN THE FOLLOWING SECTION TO SCHOOL**

----- ✂ ----- ✂ ----- ✂ ----- ✂ ----- ✂ ----- ✂ ----- ✂ -----

**ICT ACCEPTABLE USAGE AGREEMENT**

I have read and understood this ICT Acceptable Usage Agreement and I am aware of the School's ICT Acceptable Usage Policy (available on the school website) and the initiatives to maintain a cyber-safe learning environment.

Name of student ..... Class .....

Signature of student .....

Name of parent/guardian .....

Signature of parent/guardian ..... Date .....

**Please note: This agreement will remain in force as long as your child is enrolled at St. Joseph's School. If it becomes necessary to add/amend any information or rule, you will be advised in writing.**