St Joseph's School
PORT LINCOLN
In all things love

St Joseph's School
ICT Acceptable Use Policy

St Joseph's School
PORT LINCOLN
In all things love

Contents

St Joseph's School
PORT LINCOLN
In all things love

1. Purpose

The purpose of this document is to set out the School's policy regarding the acceptable use of ICT.

2. Definitions

In this policy:

- **CESA** means Catholic Education South Australia
- **CEO** means the Catholic Education Office
- **ICT** means Information and Communication Technology, which includes any facilities (whether physically at the School, in the "cloud", or elsewhere) used to compute, communicate and to store information electronically. This may include and is not limited to desktop, laptop, and tablet computers, computer servers, electronic storage devices, network and telecommunications equipment and associated software.
- **SACCS** means the South Australian Commission for Catholic Schools
- **School** means St Joseph's School Port Lincoln.

3. Scope

This policy applies to all members of the School community.

4. Policy Statement

4.1. General statement of values

The School:

- is committed to providing an **excellent education** for all students;
- recognises that **ICT is an important and powerful learning tool**, and aims to promote **safe and responsible behaviour** when using it.
- wants its students to be **confident and careful creators and users of ICT**, given that the use of technology is increasingly important;
- views the **physical and online safety** of its students and staff as being of **paramount importance**;
- expects users of ICT to **communicate** in the same **appropriate, safe, mindful, courteous manner** online as they do offline;

- encourages **efficient and timely communication**, with a focus on **environmental sustainability**; and
- strives for **operational efficiency**.

4.2. Technologies covered

The School provides Internet access, desktop computers, laptop computers and tablet devices, videoconferencing capabilities, online collaboration capabilities, message boards, and email.

As new technologies emerge, the School will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

4.3. Spirit of this Policy

All ICT provided or used by the School are intended for educational purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it:

- be safe, appropriate, careful and respectful;
- don't try to get around technological protection measures;
- use good common sense; and
- ask for help if unsure.

4.4. Privacy

An individual's School network account must be considered personal and, as such, users must respect the privacy of others by not attempting to access another user's account.

However all data, including emails that are stored on the School's ICT network (whether physically at the School, in the "cloud", or elsewhere), remain the property of the School. As such, the School reserves the right to examine any and all data on the School's ICT network and ICT devices to ensure that usage complies with the School's policies and relevant matters such as copyright and plagiarism.

4.5. Internet Access

St Joseph's School provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CESA, SACCS, CEO and School policies and procedures. The School reserves the right to monitor Internet browsing, and to retain internet activity records indefinitely.

Users are expected to respect that internet filtering is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow protocol to alert an ICT staff member or submit the site for review.

4.6. Communication

Email, SEQTA, Class Dojo, Seesaw and Microsoft Teams are used for school-related communication. Availability and use will be filtered and may be restricted based on CESA, SACCS, CEO and School policies and procedures.

Users are provided with individual accounts, which should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; and should always use appropriate language.

Users are expected to communicate in the same appropriate, safe, mindful, courteous manner online as they do offline; and usage may be monitored and archived.

4.7. Collaborative Content

The School recognizes that collaboration is an essential part of education and may sometimes require users to register with web sites or tools that allow communication, collaboration, sharing, and messaging among users.

In addition to communicating in an appropriate manner, users should be careful not to share personally-identifying information online. The School reserves the right to monitor posts, chats, sharing, and messaging.

4.8. ICT Devices provided by the School

The School may provide users with mobile computers or other devices to promote learning both inside and outside of the classroom. Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to users' care. Users should report any loss, damage, or malfunction to ICT staff immediately. The School reserves the right to hold users financially accountable for loss, damage or malfunction resulting from negligence or misuse, including by recovering the full replacement cost of devices and software.

The School also reserves the right to monitor the use of school-issued devices.

4.9. Personally-Owned Devices

Year 10 to 12 students use personally-owned devices (including laptops, tablets, mobile phones, external storage) under teacher supervision and instruction, to ensure such use does not interfere with the teaching and learning in the educational environment.

Many personal devices are internet capable. Users are not to use such devices to access the internet as a means to bypass the school's filtering and security software. Any misuse of personally-owned devices may result in disciplinary action.

Personally owned devices used on the School's premises or ICT network are covered by this policy, including the School's right to monitor the school-related use of ICT, and to inspect any data held on the device.

4.10. Security

Users are expected to take reasonable precautions against the introduction or transmission of security threats to the School's ICT network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If you believe the computer or mobile device you are using might be infected with a virus or other malware, please alert ICT department immediately. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

4.11. Downloads

Users should not download or attempt to download or run executable programs over the School's ICT network, or onto School devices, without express permission from ICT staff. Files must only be downloaded from reputable sites and only for educational purposes. If unsure seek help from ICT staff or a teacher.

4.12. Respect and Caution

Users should always ensure that they use the Internet, the School's ICT network resources and online sites in a courteous and respectful manner.

Users should also recognize that among the valuable content online there can be unverified, incorrect, or inappropriate content. Users should only use reliable sources when conducting research via the Internet.

Users should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it's out there in some form forever. It can sometimes be used and spread in ways you never intended.

4.13. Plagiarism

Users should not copy or take credit for things they didn't create themselves or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

4.14. Personal Safety

If you see a message, comment, image, or anything else online that makes you concerned for your own personal safety or that of another student or staff member, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

Users of ICT:

- should never share personal information, including phone number, address, birthday, photographs or financial information, over the Internet without adult permission;
- should never share or disclose usernames or passwords;
- should recognise that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard personal information of themselves and others; and
- should never agree to meet someone they meet online in real life without parental permission.

This is not intended to be an exhaustive list. Users should use their own good judgment when using the ICT on the School's network and generally.

4.15. Cyberbullying

Cyberbullying includes (but is not limited to) harassing, "dissing", "flaming", "gaslighting", "catfishing", denigrating, impersonating, outing, "doxing", tricking, excluding, and cyberstalking a person online. Cyberbullying will not be tolerated.

Users should not send emails or post comments with the intent of scaring, humiliating, hurting, or intimidating someone else. Often these activities take place outside of the school environment and we encourage parents to be vigilant in monitoring their child's online activity. Where such activity impacts on the teaching and learning that takes place within the educational environment, the school will take appropriate action. Engaging in these behaviours, or any online activities intended to

harm (physically or emotionally) another person, may result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime and may warrant referral to the police.

Remember that your activities are monitored and retained.

4.16. Limitation of Liability

While St Joseph's employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

To the extent possible, the School excludes all liability for damage, loss or harm to persons, files, data, hardware or property which arise in connection with the School's ICT devices and/or ICT network.

The School will not be responsible, financially or otherwise, for unauthorised transactions conducted over the school network.

4.17. Violations of this Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges
- Notification to parents
- Detention or suspension from School and School-related activities
- Legal action and/or referral to police

5. Responsibilities

The responsibility for the acceptable use of ICT is shared by all, including as follows:

5.1. Leadership staff

The School's leadership staff will, with the assistance of ICT staff:

- Make the policy and procedures accessible to all.
- Ensure that teachers are supported in implementing the School's policy effectively.
- Ensure that strategies are in place for regular monitoring, review, and evaluation of this policy.
- Continue to work with staff to develop best practice.

5.2. Teachers

The School's teaching staff will:

- Aim for continuous improvement in their use of ICT.
- Evaluate and implement new ICTs in their teaching as appropriate.
- Where applicable, work with colleagues to contribute to a coordinated approach to ICT skills teaching within year levels.
- Ensure vigilance to protect students' safety and security online.
- Educate students and parents to enable responsible and ethical use of ICT.

5.3. Students

The School's students will:

- Follow guidelines and expectations of ICT use for educational purposes.
- Follow the same rules of respect online as offline.
- Employ responsible self-management with regard to use of ICT.
- Respect that Internet filtering is a safety precaution and not try to circumvent it.
- Report any concerns for online safety (eg. Cyberbullying) to an adult.

5.4. Parents and Caregivers:

Our students' parents and caregivers will:

- Ensure they are fully informed of this policy.
- Support students with the provision of a required device (from Year 10).
- Monitor their child's ICT use.
- Use SEQTA, Seesaw and other means of electronic communication effectively, responsibly and respectfully.

6. Related Documents

The following CESA/SACCS documents should be read in conjunction with this policy:

- Building Respectful Relationships Policy
- Charter for Parents in SA Catholic Schools
- Code of Conduct Policy
- Cyber Security Framework
- Cyber Security Policy

- Cyber Incident Policy and Response Plan
- ICT Acceptable Use Policy
- ICT Acceptable Use Guidelines
- ICT Access Management Policy
- Privacy Policy
- Social Media Policy and Guidelines

The following School documents should be read in conjunction with this policy:

- Acceptable Use Agreements signed by individual students
- Privacy Policy
- Student Mobile Devices Policy
- Student Mobile Devices Breach Procedure
- Teaching and Learning Policy

7. Review

Document Date	December 2024
Review Date	December 2027
Version	2.0
Revision History	December 2024 – 2024 Document Updates July 2023 – Document Created