St Joseph’s Primary School	System Update: 01. 11. 2020	
Version 0.2	Date of Next Review: 01. 11. 2023	

Staff Digital Technology Policy & Agreement

Introduction:

St Joseph’s Primary School is committed to creating a safe and responsible attitude towards the use of digital technology and learning. The school provides staff and students with digital technology for education, communication, and research purposes. Staff members are expected to exercise responsibility, use the resources ethically, respect the rights and privacy of others and operate within the laws of the State and Commonwealth, including antidiscrimination and sexual harassment laws and other school policies.

This policy & associated agreement aims to ensure that staff members use digital technology appropriately to improve and enhance learning, teaching and communication.

St Joseph’s Primary School resources should not be used for inappropriate or improper activities including pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment, including sexual harassment, stalking, bullying, privacy violations and illegal activity, including illegal peer-to-peer file sharing.

Non-compliance with this policy will be regarded as a serious matter and appropriate action will be taken, which may include termination of employment.

Scope:

This policy applies to all users of St Joseph’s Primary School information, Communication & Technologies (ICT) resources, as defined below, located at schools, and in private homes or at any other location. This policy applies to all use of ICT resources, including, but not limited to:

- Copying, saving or distributing files;
- Data;
- Downloading or accessing files from the internet or other electronic sources;
- Electronic bulletins/notice boards;
- Electronic discussion/news groups;
- Email;
- File sharing, storage, transfer;
- Information;
- Instant messaging;
- Online discussion groups and ‘chat’ facilities;
- Printing material;
- Publishing and browsing on the internet;
- Social networking;
- Streaming media;
- Subscriptions to list servers, mailing lists or other like services;
- Video conferencing;
- Viewing material electronically.

Definitions:

Electronic Communication: email, instant messaging, virtual conferencing, social media and any other material sent electronically.

Email: The system used for the purpose of school related or other Catholic Education Commission Victoria (CECV) electronic communications. Email systems are part of the School’s ICT resources.

ICT Resources: Includes but is not limited to all networks, systems, software and hardware including local area networks, wide area networks, wireless networks, intranets, CECV email systems, computer systems, software, servers, desktop computers, printers, scanners, personal computers (desktops, notebooks and tablets), mobile phones, portable storage devices including digital cameras and USB memory sticks, handheld devices and other ICT storage devices.

Personal Use: All non-work-related use of school ICT resources including internet usage, social networking and private emails.

Users: Any person using the school’s ICT resources.

Non-Compliance:

Non-compliance with this policy will be regarded as a serious matter and appropriate action will be taken, which may include termination of employment.

Depending on the nature of the inappropriate use of the school’s ICT resources, non-compliance with this policy may constitute:

- A breach of employment obligations
- A criminal offence
- A threat to the security of Department ICT resources and information
- An infringement of the privacy of staff and other persons
- Exposure to legal liability
- Serious misconduct
- Sexual harassment
- Unlawful discrimination.

Where there is a reasonable belief that illegal activity may have occurred, this may be reported to the police.

Use of School ICT Resources:

St Joseph’s Primary School ICT resources are provided to staff members for education, communication, and research purposes. Other than limited personal use, the school’s ICT resources must be used:

- For educational communication, and research purposes only;
- Like other business resources where users must comply with any codes of conduct, ministerial orders or legislative requirements that apply to the user, such as Privacy & Data breach requirements.

Staff members are allowed reasonable access to electronic communications using the school’s ICT resources to facilitate communication between other staff members, students, parents, carers, CECV representatives and other educationally related stakeholders, provided that use is not unlawful, offensive or otherwise improper. This may also include a union on matters pertaining to the employer/employee relationship.

Staff Members must ensure that large data downloads or transmissions are minimised to ensure the performance of the school’s ICT resources for other users is not adversely affected.

Personal Use:

Staff members are permitted to use St Joseph’s Primary School ICT resources for personal reasons provided the use is not excessive and does not breach this policy.

Excessive personal use during working hours covers personal use which satisfies the following criteria:

» It occurs during normal working hours (but excluding an employee’s lunch or other official breaks);

» It adversely affects, or could reasonably be expected to adversely affect, the performance of the employee’s
duties; and
The use is not insignificant.

The school may seek reimbursement or compensation from a staff member for all or part of any costs where the user has caused the school to incur exp[enses due to excessive downloading of non-work related material in breach of this policy.

Subject to limited personal use, social networking, on-line conferences, discussion groups or other similar services or tools using the school’s ICT resources must be relevant and used only for teaching and learning purposes or professional development activities. Staff members must conduct themselves professionally and appropriately when using such tools.

Unless otherwise approved, staff member email addresses should not be used to subscribe to private subscriptions and other like services (e.g. on line ticket services, bill payments) and should never be used as “recovery email’ addresses for any other services. Subscribing to mailing lists and other like services using the school’s ICT resources must be for school related purposes or professional development only and a different password must be used for all such purposes.

Staff members should be aware that the provisions applying to access and monitoring of the school’s ICT resources also apply to personal use.

Use of Personal Devices:

St Joseph’s Primary School discourages the use of personal devices, owned by staff members, for the purpose of teaching and learning or other school related activities. The use of personal devices for a work-related purpose compromises the school’s ability to secure, monitor and control information used, stored and shared by the staff member. The use of personal devices increases the potential for the misuse, loss, unauthorised access or disclosure of school sensitive, personal or health information.

The use of personal devices also exposes the school’s ICT resources to Malware (malicious software programs designed to cause damage and other unwanted actions on a computer system eg… computer viruses, worms, spyware and trojans).

Staff members are not permitted to connect their own personal devices (computers, laptops, ipad, mobile phones) to any of the school’s ICT resources without expressed permission from the school Principal or their nominee.

The school will ensure that staff members are provided with adequate ICT resources (computers, laptops, ipad, internet & email access etc…) to enable them to effectively fulfil their role.

Furthermore, staff members who access or store personal, health or sensitive information on the personal device are in breach of the CECV & school’s Privacy & Data Breach Policies.

The use of personal devices may also expose staff members to allegations of inappropriate use or behaviour and expose them to the potential of report under the Reportable Conduct Scheme.

Defamation:

St Joseph’s Primary School ICT resources must not be used to send material that defames an individual, organisation, association, company or business.

The consequences of a defamatory comment may be severe and give rise to personal and/or school liability. Staff members are reminded that electronic communications may be easily copied, forwarded, saved, intercepted or archived. The audience of an electronic message may be unexpected and widespread.

All emails sent externally from the school’s service must be accompanied by a disclaimer attached to them. The use of the email disclaimer may not necessarily prevent the school or the sender of the email from being held liable for its contents.

Illegal Use & Materials:

St Joseph’s Primary School ICT resources must not be used in any manner contrary to law or likely to contravene the law. Any suspected offender may be referred to the police or other relevant authority and their employment may be terminated.

Certain inappropriate, unauthorised and non work-related use of the school’s ICT resources may constitute a criminal offence under the Crimes Act 1958 (Vic). Examples include computer ‘hacking’, unauthorised release of data, school material or leaking of information or documents and the distribution of malware.

Illegal or unlawful use of ICT resources includes but is not limited to:

- Use of of pornography under the Crimes Act 1958 (Vic), such as child pornography;

- Offences under the Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (Vic);
- Defamatory material;
- Material that could constitute racial or religious vilification, or unlawfully discriminatory material;
- Stalking;
- Blackmail and threats under the Crimes Act 1958 (Vic);
- Use that breaches copyright laws, fraudulent activity, computer crimes and other computer offences under the Cybercrime Act 2001 (Cth) or Crimes Act 1958 (Vic);
- Breaches under any other relevant legislation.

In particular, child abuse material represents the antithesis of the school's responsibilities with regard to the safety, welfare and education of children. Any suspected offender will be referred to the police and their employment will be terminated if the allegations are substantiated.

Offensive or Inappropriate Materials:

The school's ICT resources must be appropriate to a workplace environment and aligned to school's values. This includes, but is not limited to the content of all electronic communications, whether sent internally or externally.

St Joseph's Primary School ICT resources must not be used for material that is pornographic, harassing, hateful, racist, sexist, abusive, obscene, discriminatory, offensive or threatening. This includes sexually-oriented messages or images that could constitute sexual harassment.

Staff members who receive unsolicited, offensive or inappropriate material electronically should delete it immediately and may choose to notify their principal or immediate manager of such instances. Where the sender of this material is known to the user, the user should notify the sender to refrain from sending such material again.

Offensive or inappropriate material must not be forwarded internally or externally, or saved onto school ICT resources, except where the material is required for the purposes of investigating a breach of school policies.

Confidentiality & Privacy:

Electronic communication is not a secure means of communication. While every attempt is made to ensure the security of the school's ICT resources, this security is not guaranteed, particularly when communicated to an external party. Staff members should consider the confidentiality of the material they intend to send when choosing the appropriate means of communication.

The School will handle any personal information collected through the use of the school's ICT resources in accordance with the school's Privacy & Data Breach policies.

Access & Monitoring:

The school Principal, their nominee or authorised person/s may access or monitor the school’s ICT resources at any time without providing notice to the users. This includes, but is not limited to, use of the school email systems, and other electronic documents and records and applies to the use of the school’s ICT resources for personal use.

However, school Principal, their nominee or authorised person/s must have a valid reason for accessing or monitoring the use of school’s ICT resources and are required to maintain a log recording relevant details of the access and monitoring activity.

The school Principal, their nominee or authorised person/s may access or monitor the records of the school’s ICT resources for operational, maintenance, compliance, auditing, legal, security or investigative purposes. Electronic communications that have been sent, received or forwarded using school’s ICT resources, may be accessed and logs of websites visited may be examined and monitored.

If there is a reasonable belief that the school’s ICT resources are being used in breach of this policy, the Principal or their nominee may secure the staff member, suspected of inappropriate uses, equipment while the suspected breach is being investigated.

The Principal or their nominee may also suspend a staff member’s use of school ICT resources.

School Property:

Electronic communications created, sent or received using the school email systems are the property of the school and may be accessed by the Principal, their nominee or authorised person/s in the case of an investigation. This includes investigations following a complaint or investigations into misconduct.

Electronic communications may also be subject to discovery in litigation and criminal investigations. All information produced on users’ computers, including emails, may be accessible under the Freedom of Information Act 1982 (Vic).

Email messages may be retrieved from back-up systems.

References:

Australian Commonwealth Government - *Cybercrime Act 2001;*

Australian Commonwealth Government - *Offences under the Classification (Publications, Films and Computer Games) (Enforcement) Act 1995;*

Australian Commonwealth Government - *Privacy Act 1998;*

Office of the Australian Information Commissioner (OAIC) - *Australian Privacy Principals 2014*

Office of the Australian Information Commissioner (OAIC) - *Data Breach Notification Guide: A Guide to Handling Personal Information Security Breaches 2018;*

Victorian Government, Education Department & Training – *Acceptable Use Information and Communications Technology Resources 2018;*

Victorian Government – *Crimes Act 1958.*

Staff Digital Technology Agreement

Acknowledgement

I understand that the use of St Joseph’s Primary School’s ICT Resources and digital network is subject to the terms outlined in the school’s *Staff Digital Technology Policy.*

I agree that I have read and understand the terms and conditions and will agree to abide by it at all times.

Name:
Signature:
Date:

Principal / Nominee:
Signature:
Date: