Floreat Park Primary School

An Independent Public School
e-Safety Policy

Ratified by	Date
School Board	19 March 2019
Review Date	March 2021

Digital Technologies/e-Safety Policy 2018

1. Vision

1.1. To create a safe and engaging environment in which students can communicate, investigate and create with ICT in meaningful, social and ethical ways.

2. Purpose and Rationale

2.1. Staff and students at Floreat Park Primary School (FPPS) use the digital technologies as a valuable teaching, learning and communication tool. The use of digital technologies and information and communication technology is an integral aspect of our daily lives and will be a core aspect of our students' future. However, we acknowledge that there are particular risks associated with digital technologies and they must be used responsibly.

2.2. Digital technologies provide students with unprecedented opportunities to obtain information, engage in discussion and liaise with individuals, organisations and groups worldwide, so as to increase skills, knowledge and abilities.

2.3. Through the teaching of ICT (Information and Communication Technologies), Digital Technologies and Protective Behaviours, we aim to develop every student's ability to use and manage digital technologies effectively whilst using a high degree of social and ethical protocols.

3. Aims

- To develop student skills and attitudes in the safe and appropriate use of digital technologies.
- To develop students who demonstrate a high level of social and ethical protocols when using technology.

4. Implementation 'A, B, C'

4.1. We acknowledge that the nature of the digital technologies including the Internet means that full protection from inappropriate content via filtering software can never be guaranteed. Therefore, we follow a holistic **'A, B, C'** approach:

A: **Access** – filtering systems and controls

B: **Boundaries** – Polices and expectations

C: **Communication** – Education and support for students, parents and staff

Access: How we control and filter access to the internet for students and staff

4.2. The Department of Education (DoE) requires that all public schools operate their technologies under a 'Standard Operating Environment' (SOE).

4.3. Every student from Year 2 logs on using their username and password. These are managed through the Department Account Manager (DAM) tool.

4.4. All internet traffic is decrypted and routed through the DoE firewall. The school has some control over the firewall and is able to monitor what sites or internet services students are accessing. The school will continue to ensure that it is accessing the highest level of filtering available from and supported by the DoE.

4.5. The school employs a part time 'Panel Integrator' (ICT technician) from a company on the DoE list of approved contractors. This ensures that our systems are maintained to the levels and standards expected by the DoE. The technician is line managed by the Deputy Principal responsible for ICT.

4.6. The school has some control over content filtering and is able to make decisions about access to services such as YouTube, social media and cloud storage. By default, students do not have access to these platforms.

Boundaries: The policies and expectations in place.

4.7. The following DoE policies apply to staff and students: Students Online Policy, Telecommunications Policy, Code of Conduct, Student Behaviour in Public Schools Policy and Procedures, Child Protection.

4.8. The FPPS e-Safety policy is reviewed annually and amended as necessary. Related school policies and guidelines include: Mobile Devices Policy, Behaviour Engagement Policy, Technology Contract – Acceptable Use Policy, Whole School Practices with ICT (guidelines), Dealing with Online Incidents Affecting Students (guidelines).

4.9. Each student and their parents or caregivers are asked to agree to use digital technologies responsibly at school by completing the Technology Contract – Acceptable Use Policy. The Contract is reviewed regularly by class teachers and re-signed on an annual basis. This contract is available on the school website/Connect to facilitate further discussion with children at home. In school, the contract is visible in classrooms and referred to regularly.

4.10. The school has agreed whole school practices with *ICT (See Appendix A)* These include guidelines for staff to follow before, during and after technology use.

4.11. Technology at Floreat is used as a directed and purposeful learning tool only. Students are not allowed 'free access' to technology.

4.12. The ICT committee meets each term to review digital technologies usage across the school and plan for the future.

Communication: How we communicate and educate about the responsible and safe use of technology to students, staff and the community.

Students

4.13. Each class has the Technology Contract (*Appendix B*) displayed in a prominent place for students and teachers to refer to.

4.14. ICT is used to support learning across many curriculum areas. Teachers constantly reinforce the importance of safe and respectful use of technology and the Internet whenever it is used. *(See Whole School Practices with ICT Appendix A)*

4.15. Through the ICT, Digital Technologies and Protective Behaviours curricula we aim to develop every student's ability to use and manage technology whilst exercising a high degree of social and ethical protocols.

4.16. Staff remind all students to be responsible for notifying their teacher of any inappropriate material so that access can be blocked. We reassure students that they will not be 'in trouble' for telling staff if they see, or do something wrong.

Staff

4.17. Staff will receive ongoing training in the safe use of ICT with students. This is delivered face to face (through staff meetings and Professional Learning Community (PLC) meetings), via memos and email updates and through school-wide communication (DoE Connect).

4.18. Staff teach ICT skills and knowledge using the Western Australian Curriculum, ICT Capability *(Appendix C)*. This outlines the age appropriate expectations in relation to the 5 'Organising Elements': Social and Ethical Protocols, Managing and Operating, Creating, Communicating and Investigating with ICT.

4.19. Classrooms will have the Technology Contract displayed in a prominent position so that it can be referred to and discussed regularly.

4.20. If there is any concern or suspicion of inappropriate behaviour, staff must notify a member of the administration team immediately. (See Appendix D)

4.21. Guidance documents are created as and shared with staff as needed to support their practice.

4.22. Where the administration team is made aware of suspected inappropriate content or behaviour, they will investigate, inform parents and work collaboratively to address the matter in the best interests of the child(ren) involved.

4.23. In online publications (e.g. Newsletters) FPPS recognises and respects the privacy of students, parents, staff and others at all times. When identifying students, only the student's first name will be used.

Parents and Caregivers

4.24. The school will maintain an up-to-date cyber safety section on the school website/Connect with information and links for parents.

4.25. Cyber Safety parent workshops will be held at the beginning of each year, led by external experts in the field.

4.26. The Technology Contract will be available on the school website so that parents can reinforce it at home.

4.27. Parents will be informed of all suspected online incidents relating to their child(ren) so that a collaborative approach can be put in place to support the child(ren).

Whole School Practices with ICT

Before using technology	Whilst using technology	After using technology
Ensure every child and parent has signed the technology contract	If a relief teacher is unfamiliar with the class, students should not use devices*	Teach students how to take out and put away technology responsibly
A3 Technology contract on display in every classroom	Refer students to the class copy of the technology contract and remind them of the purpose for using technology in the lesson	Regularly check search history and background apps left open on iPads
Cyber safety display board in each class (age-appropriate)	Consider grouping of students, levels of responsibility and proximity to you	Report any technical issues in the ICT book
Age-appropriate cyber safety themed lesson at the beginning of each term	iPads should remain flat on desks so that teacher can see screens	Ensure technology is stored securely
Remove bottles/food from being near technology	All students should use technology only under direct supervision of the teacher	Inform admin immediately if you have any concerns
Maintain record of which students use which iPads (PP and Y1 only)	Be vigilant and regularly check in on student ICT activity	Always ask for training, guidance and support if you need it
	Remind students how to handle the technology appropriately (2 hands whilst carrying)	

*Liaise with your line manager

Kindergarten to Year 2 Technology Contract – Acceptable Use Policy

My child agrees to follow the rules set out below when using the technology devices at school:

- I will get adult permission before I use an iPad, computer or SmartBoard (device).
- I will inform a teacher if I see something that makes me uncomfortable.
- I will not eat or drink when using my device.
- I will take care of all computer equipment.
- My hands will be clean when I use my device.
- I will not change the device settings.
- I will not try to download or remove any apps or programs from the device.
- I will be responsible and use smart learning choices while using school devices.
- I will only use the device for what the adult has as asked me to do.

I understand that if I break the rules:

- The school will inform my parents and decide upon appropriate action to help me stay safe and make good choices.

---✂--

Kindergarten to Year 2 Technology Contract

I agree for my child to abide by the Technology Use Contract.

Name of Student: _____

Room: _____   Year:_____

Signature of Parent: _____

Name of Parent: _____

Date: _____

Year 3 to Year 6 Technology Contract – Acceptable Use Policy

I agree to follow the rules set out below when using technology devices at school:
- I will seek permission before I use an iPad, computer or SmartBoard (device).
- I will follow all teacher instructions when using the device.
- I will not share my password with other students or let other people login to my account.
- I will inform a teacher if I think someone is using my account.
- I am responsible for anything that happens when my account is used.
- I will inform a teacher immediately if I see something that makes me feel uncomfortable or is inappropriate for children.
- I will only use the internet if I have gained teacher permission first.
- I will not attempt to access sites that are blocked or that I have been told not to access.
- I will not access social media sites whilst at school or when using a school device.
- If I download and use pictures by others, I will cite the source.
- I will not give out my name, phone number, address, the name of the school or any photographs without checking with a teacher.
- I will take care when handling of all the equipment.
- I will not change any device settings, or download programs without permission.
- I will ensure that anything I published is polite, carefully written and well presented.

I understand if I break the rules:
- I will be held responsible for my actions or another person using my account.
- The school will inform my parents and decide upon appropriate action to help me stay safe and make good choices.

--✂--

Year 3 to Year 6 Technology Contract

I agree to abide by the Technology Use Contract.

Name of Student: _____

Signature of Student: _____

      Room: _____   **Year:**_____

Signature of Parent: _____

Name of Parent: _____

Date: _____

The Western Australian Curriculum

General Capabilities

ICT Capability and Scope and Sequence (Hyperlink)

Click the link above for the most up-to-date version

Alternatively, visit

https://k10outline.scsa.wa.edu.au/home/teaching/general-capabilities-over/information-and-communication-technology-ict-capability/

Appendix D

Guidelines for Responding to Online Incidents Affecting Students

Step 1 Identification	Step 2 Conceptualisation	Step 3 Support & Management	Step 4 Support & Follow-up
Identify and report concerns/suspicions	Gain an understanding of why and how	Review processes and take action where necessary	Provide ongoing support
Inform a member of the administration team as soon as possible and before speaking to the student(s). The administration team will coordinate the investigation into the concerns and communicate with parents. Collaboratively planning our response to cyber safety incidents will support students in learning to inform us and stay safe in the future.	The administration team, teachers, parents, school psychologist and the student(s) involved will work together to understand why and how the incident occurred. The student will be reassured and supported as it is vital to reinforce the importance of being open and telling someone. In cases where it is a repeat incident, sanctions and restorative behaviours will be agreed with student(s) and their parents.	In collaboration with the student(s) involved and their parents, put into place a plan to support the child(ren) in future. Plan support for the student(s). Children may feel distressed by events including cyberbullying, exposure to pornographic material or breaches of the school Technology Contract or Behaviour and Engagement Policy Review A, B, C to identify whether changes are required in; **A** – Access, **B** – Boundaries or **C** – Communication.	Agree on check in times and maintain open communication with parents to track the child(ren)'s behaviour in and out of school. Provide mentoring or psychological support if appropriate. Signpost parents and teachers to appropriate material to use to support the child(ren).

Based in part on the document by the Victorian State Government: Education and Training called 'The Step-by-Step Guide: Online Incidents of Inappropriate Behaviour Affecting Students'

Created with advice from ySafe - Social Media & Cyber Safety Experts