



***Floreat Park Primary School** | An Independent Public School*

e-Safety Policy

RATIFIED BY

DATE

SCHOOL BOARD

MARCH 2022

REVIEW DATE

MARCH 2023





e-Safety Policy

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 upholding 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** – Policies and expectations
 - C: Communication** – Education and support for students, parents and staff

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

- 4.2. The Department of Education (DoE) requires that all public schools operate supported technologies in schools under a 'Standard Operating Environment' (SOE).
- 4.3. Every student from Year 2 up 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 Principals.
- 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.
- 4.7. Students do have access to department authorised platforms such as Office 365.
- 4.8. All 'third party services' are assessed by the DoE and given a risk rating. The school must adhere to this rating and inform parents/seek parental permission accordingly.

iPads (school owned and parent funded)

- 4.9. All iPads are managed using Apple School Manager and JAMF.
- 4.10. Following community consultation, the Future Technologies Committee opted



to follow a model whereby iPads were managed and supervised. This means the following:

- 4.10.1. Apple School Manager allows the school to purchase apps in bulk and access special educational pricing. It removes the requirement for parents to purchase apps and install them at home.
- 4.10.2. JAMF is a mobile device management platform that allows us to set parameters around the settings such as hiding messaging, the app store and Facetime. It also allows us to define which apps appear on the iPads.
- 4.10.3. Whilst JAMF does allow some filtering of inappropriate material, parents are reminded that they must have internet filtering in place at home if their children are using the devices.



Boundaries: The policies and expectations in place.

- 4.11. 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.
- 4.12. 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).
- 4.13. Each student and their parents or caregivers are asked to agree to use digital technologies responsibly at school by completing the Technology Contracts. The contracts are tailored to K-2 and 3-6, recognising that the 1:1 program requires additional consideration.
- 4.14. 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.
- 4.15. Technology at Floreat is used as a directed and purposeful learning tool only. Students are not allowed 'free access' to technology.
- 4.16. The Future Technologies Committee is responsible for the ongoing review of digital technologies usage across the school future planning.



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

Students

- 4.17. Each class has the Technology Contract displayed in a prominent place for students and teachers to refer to. For Year 3-6 students this is in their school diary.
- 4.18. ICT is used to support learning across many curriculum areas. Teachers regularly and consistently reinforce the importance of safe and respectful use of technology and the Internet whenever it is used.
- 4.19. 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.
- 4.20. 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

- 4.21. 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), online virtual classrooms, via memos and email updates and through school-wide communication (DoE Connect).
- 4.22. Staff teach ICT skills and knowledge using the Western Australian Curriculum, ICT Capability. 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.
- 4.23. Classrooms will have the Technology Contract displayed in a prominent position so that it can be referred to and discussed regularly.
- 4.24. If there is any concern or suspicion of inappropriate behaviour, staff must notify a member of the administration team immediately.
- 4.25. Guidance documents are created and shared with staff as needed to support their practice.
- 4.26. 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.
- 4.27. 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

- 4.28. The school will maintain an up-to-date cyber safety section on the school website/Connect with information and links for parents.
- 4.29. Cyber Safety parent workshops will be held at the beginning of each year, led by external experts in the field.
- 4.30. The Technology Contract will be available on the school website so that parents can reinforce it at home.
- 4.31. 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).