| An Independent Public School

e-Safety and Mobile Devices Policy

Floreat Park Primary School

RATIFIED BY	DATE
SCHOOL BOARD	July 2023
REVIEW	June 2024

This policy outlines how we ensure the safe, respectful, and educational use of mobile and digital devices at Floreat Park Primary School. It is designed to guide students, staff, and families in supporting effective digital learning.

1 Vision

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

2 Purpose and Rationale

2.1. Staff and students at Floreat Park Primary School (FPPS) use 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 can be particular risks associated with digital technologies and they must be used responsibly.

2.2. Digital technologies provide students with unprecedented opportunities to obtain information and increase knowledge and skills by engaging in discussion and liaising with individuals, organisations and groups worldwide.

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.

2.4 FPPS has a 1:1 iPad program from Year 3-6 and students are expected to bring the device to school each day and return home with it.

2.5 Parents will be asked to sign a permission form to indicate they allow their children to bring a personal mobile device to school and that they understand and will abide by the school and Department of Education policy.

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 technologies

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 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 3 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's 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 but the DoE The technician Is line managed but the Deputy Principals.

4.6 The school has some control over content filtering at school and is able to make decisions about access to services such as You Tube, 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 part services an assessed by the Department give a risk rating. School must adhere to this rating and inform parents/seek parental permission accordingly.

iPads (school owned and parent funded)

4.9 All Pads 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:

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 storeand 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 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 Policy.

4.12. The FPPS e-Safety and Mobile Devices 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 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 school runs cyber safety sessions for parents at least once per year. These sessions are delivered by industry experts in cyber safety.

4.17. 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

4.18. Each class has the Technology Contract displayed in a prominent place for students and teachers to refer to. Teachers keep signed copies of Technology Contracts on file for duration of the year.

4.19. ICT is used to support learning across many curriculum areas. Teachers regularly and consistently reinforce the importance of safe and respectful useof technology and the Internet whenever it is used.

4.20. 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.

4.21. 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 somethingwrong.

Staff

4.22. 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).

4.23. 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.

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

4.25. If there is any concern or suspicion of inappropriate behaviour, staff notify a member of the administration team immediately.

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

4.27. 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.

4.28. 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

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

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

4.31. The Technology Contract will be available on the school website so that parents to use at home.

4.32. 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).

Acceptable Use of Mobile Devices (Part 2)

1. Purpose and Rationale

1.1 The widespread ownership of mobile phones and wearable devices (collectively "mobile devices") among students requires that school administrators, teachers, students, and parents take steps to ensure that such technology are used responsibly at school. This policy is designed to ensure that potential issues involving personal devices can be clearly identified and addressed, ensuring the benefits that personal devices can provide (such as increased safety) can continue to be enjoyed by our students.

1.2 The Department of Education has a policy on Student Mobile Phones in Public Schools. It states that student use of mobile phones in public schools is not allowed, unless for medical or teacher directed educational purpose. The policy can be found here.

1.3 FPPS has established this policy for personal devices that provides teachers, students and parents guidelines and instructions for the appropriate use of personal devices during school hours. The policy is in line with the Department of Education Policy on Student Mobile Phones in Public Schools February 2020 (V1.2).

1.4 Floreat Park Primary School (FPPS) accepts that parents give their children personal devices to protect them from everyday risks involving personal security and safety. Parents may also be concerned about children travelling alone on public transport or commuting long distances to school. It is acknowledged that providing a child with a personal device gives parents reassurance that they can contact their child if they need to speak to them urgently.

1.5 This policy for personal devices also applies to students during school excursions, camps and extra-curricular activities when under the supervision of school staff.

1.6 FPPS has a 1:1 Technology Program (iPad) which is used for teaching and learning purposes.

2. Responsibilities

Students, Parents and Caregivers

2.1 Students and their parents or caregivers should read and understand this policy before their children are permitted to bring their personal phones/devices to school.

2.2 It is the responsibility of students who bring personal devices to school to abide by the guidelines outlined in this policy.

2.3 The decision to provide a personal device to their child should be made by parents or caregivers.

2.4 Parents should be aware that if their child takes a personal device to school, FPPS accepts no responsibility for loss or damage caused to the device. The school recommends AppleCare+ or personal insurance to cover devices including iPads.

2.5 The school will take all reasonable steps to minimise the risk of devices being lost/damaged:

(a) Mobile phones/smart watches will be kept secure in the classroom out of sight during the day

(b) iPads should have cases to minimise the impact of being dropped

(c) Students will be trained and reminded to transport the iPads carefully in two hands

(d) iPads will be moved from bags to the classroom at the start of the day to minimise the risk of being damages/lost from bags. iPads will be placed in bags at the end of the day and students are reminded that they should not be removed until they are home

(e) iPads are managed by the school Mobile Device Management (MDM) software. When connected to a Wifi, MDM can be used to track/lock or wipe an iPad remotely

(f) The MDM also allows the school to hide apps such as messages, the App storeand social media apps at school AND home

(g) The school is responsible for filtering the internet connection on the schoolsite but cannot filter home internet or public Wi-Fi

3. Acceptable Use of Personal Devices at School

Personal devices include the following:

- Mobile phones
- Portable hotspots or devices capable of 'hot spotting'
- Tablets/laptops
- Wearable devices and MP3 players that have:
  - a SIM card that connects to the internet;
  - Wi-Fi/Bluetooth connectivity;
  - the ability to capture or record sounds or images; and
  - Can be used to communicate with devices outside the school

Examples of wearable devices that are not allowed include Internet enabled watches such as Apple watches, certain Fitbit models, vTech models.

Spacetalk watches are suitable so long as 'school mode' is enabled. In the case that a Spacetalk watch is being used inappropriately at school, the watch will be treated as a wearable internet able device. It'll be removed and parents contacted.

Using personal devices responsibly at school:

3.1 Mobile phones or other mobile devices should not be used by students during school hours (8:50am-3:10pm) unless authorised by a member of the administrativeteam.

3.2 1:1 iPads should remain in school bags from when a student leaves home until the beginning of lessons at school. At the end of the school day, iPads should be placed in bags and remain there until the student arrives home.

3.3 Parents who need to contact their child should do so by calling the main school phone number.

3.4 If exceptional circumstances exist, parents should agree communication protocolswith a member of the administration team.

3.5 While at school personal devices should be switched off and handed in to the class teacher.

3.6 Mobile devices are not to be used in any situation that may cause embarrassment or discomfort to their fellow students, staff or visitors to the school.

3.7 Students are reminded to protect their phone numbers, email addressed and social media details by only giving them to close friends and family. It may help younger students to keep a note of who they have given their phone number to. This can help protect the student's number from falling into the wrong hands and guard against cyber-bullying.

Cyber Safety

3.8 Students are taught cyber safety throughout the year as part of the ICT General Capability in the West Australian Curriculum. Cyber safety is also addressed during teaching of Protective Behaviours. See e-Safety and Mobile Devices Policy Part 1 – for more information.

Cyberbullying:

3.9 Using mobile devices to bully (also known as cyberbullying) and threaten other students is unacceptable and will not be tolerated. In some cases, can constitute criminal behaviour. Please refer to the Behaviour Engagement and e-Safety Policies as well as relevant Department of Education policies and guidelines.

3.10 Students, parents and caregivers are reminded that it is a criminal offence to use a mobile phone to menace, harass or offend another person and calls, text messagesand emails can be traced.

3.11 Mobile phones or other mobile devices must not be used to take photos/video of anyother student or teacher without their consent. It is also prohibited to upload photos/video of other students/teachers to social media websites or email photos/videos to others without their explicit permission.

Theft or damage:

The school takes no responsibility for the damage or loss of mobile devices unless there is evidence of negligent behaviour.

3.12 Parents and caregivers are encouraged to mark their child's mobile device(s) clearly so that they can be identified. All students are advised to have their name and another contact number stored on the phone so that it can be more easily returned if lost.

3.13 All 1:1 iPads are registered in the MDM and traceable when connected to Wifi.

3.14 Students who bring a mobile device to school should hand it in to the class teacherupon arrival at school.

3.15 Mobile devices that are found in the school and whose owner cannot be located should be handed to the school office.

3.16 FPPS accepts no responsibility for replacing lost, stolen or damaged mobile devices.

3.17 FPPS accepts no responsibility for students who lose or have their mobile devices stolen while travelling to and from school. Students are encouraged to keep phonesand devices out of sight on the way to and from school.

3.18 Students should use passwords/pin numbers to ensure that unauthorised access to their device is not possible.

3.19 Students must keep their password/pin numbers confidential. This is part of the technology contract.

3.20 The school has the ability to reset student passwords on 1:1 iPads and Department of Education accounts.

3.21 If a mobile phone is lost or stolen, parents and students are advised to report the loss/theft to their service provider so that they can de-activate the SIM card and block the mobile phone from use across all networks. Blocking a lost/stolen phonewill make it unusable to anyone else within Australia.

4. Consequences of unacceptable/inappropriate use

Also refer to the Student Engagement Policy for managing behaviour matters

4.1 Any inappropriate use of mobile devices must be reported immediately to theschool leadership team.

4.2 Students using mobile devices contrary to the agreed ways set out in this policy will face disciplinary action as sanctioned by the school's administration. This will in all cases include consultation with parents or caregivers.

4.3 Repeated infringements may result in the withdrawal of the agreement to allow the student to bring the mobile telephone to school.

Appendix A

STUDENT MOBILE PHONES IN PUBLIC SCHOOLS POLICY EFFECTIVE: 3 FEBRUARY 2020