Inglewood Primary School

Responsible Use of Internet and Mobile Devices *Guidelines*

Together we nurture inspired, curious and confident learners.

Responsible Use of Internet and Mobile Devices Guidelines

Rationale

With the widespread use of personal digital devices (including mobile phones and wearables), it is essential that students, staff, and families work together to ensure responsible use at school. This policy outlines our approach to the safe, respectful, and educational use of digital technologies, supporting effective learning in line with our school values: Respect, Integrity, Perseverance, and Kindness.

Digital technologies are a vital part of teaching, learning, and communication at Inglewood Primary School. While they offer valuable opportunities for collaboration and knowledge-building, we recognise the need to manage associated risks. Through ICT, Digital Technologies, and Protective Behaviours education, we aim to equip students with the skills to use technology ethically and effectively.

This policy provides clear guidelines for the appropriate use of personal devices during school hours, excursions, camps, and extra-curricular activities. It aligns with the Department of Education's Student Mobile Phones in Public Schools Policy (Feb 2020, V1.2).

Inglewood Primary School has a 1:1 Program (iPad) in Year 4-6, which is used for teaching and learning purposes. Students are expected to bring the device to school each day and return home with it.

We acknowledge that the nature of 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:
Access - Filtering systems and controls
Boundaries - Polices and expectations
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.

- The Department of Education (DoE) requires that all public schools operate supported technologies in schools under a "Standard Operating Environment (SOE).
- Every student from Year 4 logs on using their username and password. These are managed through the Department Account Manager (DAM) tool.
- All internet traffic is decrypted and routed through the DoE firewall. The school has some control over the firewall and can 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.
- 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 by a Deputy Principal and the Manager of Corporate Services.
- The school has some control over content filtering at school and can restrict access to services such as YouTube, social media, and cloud storage. By default, students do not have access to these platforms.
- Students do have access to department authorized platforms such as Office 365; this is provided by DoE.
- All third-party services are assessed by the Department and given a risk rating. The school must adhere to this rating and inform parents/seek parental consent accordingly.

iPads (school owned and parent funded)

All Pads are managed using Apple School Manager and JAMF (from 2026 for parent funded devices) while connected to the school's internet service. JAMF is a mobile device management platform that allows the school to set parameters around settings such as hiding messaging, the app store and Facetime. It also allows us to define which apps appear on the iPads. Whilst JAMF does provide 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.

- The Inglewood Primary School Internet Use and Mobile Devices Guideline is reviewed every two years and/or amended, as necessary. Related school policies and guidelines include Responsible Behaviour and iPromise student contract.
- Upon enrolment, parents or caregivers provide permission for an online services account.
- Each student and their parents or caregivers are asked to agree to use digital technologies responsibly at school by completing the iPromise contracts. The contracts are tailored to K-3 and 4 -6, recognising that the 1:1 program requires additional consideration.
- The iPromise 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.
- Technology at Inglewood is used as a directed and purposeful learning tool only. Students are not allowed 'free access' to technology.
- The school runs cyber safety sessions for parents at least once per year. These sessions are delivered by industry experts in the digital technologies area.
- Teachers from Years 4-6 use Apple Classroom to manage students iPad use, and all teachers are diligent in checking students' use of the iPads.

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

Students

- Each class has the iPromise Contract displayed in a prominent place for students and teachers to refer to.
- 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.
- Through the ICT, Digital Technologies and Protective Behaviours curricula we aim to develop every student's ability to use and manage technology in a safe and respectful way.
- Staff remind all students to be responsible for notifying their teacher of any inappropriate material so that access can be blocked.

Staff

- Staff will receive ongoing training in the safe use of ICT with students. This is delivered face to face, online virtual classrooms, via memos and email updates and through school wide communication.
- Staff teach ICT skills and knowledge using the Western Australian Curriculum, ICT Capability.
- Classrooms will have the iPromise contract displayed in a prominent position so that it can be referred to and discussed regularly.
- If there is any concern or suspicion of inappropriate behaviour, staff notify a member of the administration team immediately.
- Guidance documents are created and shared with staff as needed to support their practice.

Responsibilities

Students, Parents and Caregivers

- 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.
- It is the responsibility of students who bring personal devices to school to abide by the guidelines outlined in this policy.
- The decision to provide a personal device to their child should be made by parents or caregivers.
- Parents should be aware that if their child takes a personal device to school, IPS accepts no responsibility for loss or damage caused to the device. The school recommends AppleCare+ and families to check their personal insurance to cover devices including iPads.

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

- Mobile phones/smartwatches should be kept secure in the classroom out of sight during the day.
- iPads must have cases to minimise the impact of being dropped
- Students will be trained and reminded to transport the iPads carefully in two hands. Students are to bring their iPads to school in their school bags and iPads will be moved from bags to the classroom at the start of the day to minimise the risk of being damaged/lost. iPads will be placed in bags at the end of the day and students are reminded that they are not to be removed until they are home.

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

- The MDM also allows the school to hide apps such as messages, the App store and social media apps at school.
- The school is responsible for filtering the internet connection on the school site but cannot filter home internet or public Wi-Fi.

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 and 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 will be held in the office and returned at the end of the day, with parents being contacted.

Using personal devices responsibly at school:

- The school strongly discourages students from bringing mobile phones, other connected devices and smart watches to school. Students are able to contact their parents via email or on the school phone.
- Mobile phones or other mobile devices such as connected devices and smart watches should not be used by students during school hours (8:30am-3:00pm).
- 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.
- Parents who need to contact their child should do so by calling the main school phone number.
- If exceptional circumstances exist, parents should agree communication protocols with a member of the administration team.
- While at school personal devices (mobile phones) should be handed in to the class teacher who will store them safely.
- Students are reminded to protect their phone number and email address 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

Students are taught cyber safety throughout the year as part of the ICT General Capability in the Western Australian Curriculum. Cyber safety is also addressed during the teaching of Protective Behaviours.

Cyberbullying:

- Using mobile devices to bully (also known as cyberbullying) and threaten other students is unacceptable and will not be tolerated. In some cases, it can constitute criminal behaviour. The school will work with families and any appropriate agencies when cyber bullying is evident.
- Mobile phones or other mobile devices must not be used to take photos/videos of any other 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.
- 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.
- From 2026, All 1:1 iPads are registered in the MDM and traceable when connected to **Wi-Fi.**
- Students who bring a mobile device to school must hand it in to the class teacher upon arrival at school.
- Mobile devices that are found in the school and whose owner cannot be located should be handed to the school office.
- Inglewood Primary School accepts no responsibility for replacing lost, stolen or damaged mobile devices.
- Inglewood Primary School accepts no responsibility for students who lose or have their mobile devices stolen while travelling to and from school. Students are encouraged to keep phones and devices out of sight on the way to and from school.
- Students should use passwords to ensure that unauthorized access to their device is not possible.
- Students must keep their password confidential. This is part of the iPromise contract.
- The school can reset student passwords on 1:1 iPads and Department of Education accounts.
- 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 deactivate the SIM card and block the mobile phone from use across all networks. Blocking a lost/stolen phone will make it unusable to anyone else within Australia.

Consequences of unacceptable/inappropriate use

- Any inappropriate use of mobile devices must be reported immediately to the school leadership team.
- Students using mobile devices contrary to the agreed ways set out in this policy will receive an appropriate consequence and will, in all cases, include consultation with parents or caregivers.
- Repeated infringements may result in the withdrawal of the agreement to allow the student to bring the mobile device to school.

Escalation process for misuse of digital technologies *(Including mobile phones)*

If a student is seen misusing a device including online use with a med/high level behaviour it will be reported to a member of admin, by the teacher immediately. Admin will follow the Responsible Behaviour Guidelines as appropriate. The following escalation process will be followed specifically for digital technologies misuse:

Low Level
1. Verbal Warning
2. Loss of access to the device for one lesson

Medium Level
3. Loss of access to the device for one day

High Level
4. Loss of access to the device for one week
5. Loss of access to the device for the remainder of the term/year

Examples of low-level misuse that may result in loss of access:
- Time wasting (i.e. taking selfies when not required as part of the task, playing music etc.)
- Plagiarism of online content
- Unauthorized access of online sites (i.e. YouTube - of a low-level nature); and
- Leaving your device unattended.

Examples of medium level misuse that may result in loss of access:
- Downloading apps without permission
- Changing settings without permission
- Plagiarism of online content (medium level)
- Accessing inappropriate material (medium level)
- Misusing other people's images/property; and
- Using the iPad in a careless way (physical).

Examples of high-level misuse that may result in loss of access:
- Using another student's device or ID without permission
- Intentionally damaging a device
- Accessing inappropriate sites (high-level)
- Bullying or intimidating other people online.

Attachments:

iPromise 2026

Review Date: September 2027.

Inglewood Primary School
Student Agreement for Using a Personal iPad

2026 1:1 iPad Promise

iPromise to

- take good care of my iPad;
- only use my iPad with **my teacher's permission;**
- use my iPad purely for educational purposes **as instructed by my teacher;**
- follow the Inglewood Primary School iPad Code of Conduct**;**
- use my iPad's camera and audio recorder **only when I have my teacher's permission;**
- understand that my iPad is subject to inspection at any time;
- connect to Apple Classroom in all classes in which they are using their iPad;
- charge my iPad every night and bring it to school each day;
- abide by the **iPromise Details** (*that form part of this agreement*).

Date: _____

Student Name (please print): _____

Student Signature: _____

*I understand and support the 1:1 iPad **iPromise** made by my child. I am aware of my responsibilities in relation to maintenance and care of the iPad. I have read and understand the 1:1 iPad **iPromise – details**, supplied with this agreement.*

Parent/Carer Name: (please print): _____

Parent/Carer Signature: _____

Scan for digital version

1:1 iPad iPromise – details

(What it means for Teachers, Students and Parents)

Teachers will:

- ensure that students in their class have been given permission by the leadership team before they access their iPad at school;
- supervise students when using iPads;
- Use Apple Classroom to monitor students iPad activity during class.
- monitor student use of apps;
- communicate with parents to show how the iPads are integrated into teaching and learning;
- inform parents of any misuse of the iPad.

Students will:

- be responsible for their own iPad.
- ask permission before accessing their iPad.
- ensure their iPad is charged for the start of each school day.
- leave their iPad charger at home to recharge their iPad each night.
- store and always transport their iPad in a suitable case.
- always leave their iPad in the classroom until the end of the school day.
- ensure that their security codes are kept private from other students.
- show care and respect for their iPads and those of others.
- notify the teacher if the iPad is broken or fails to work properly.
- only use their iPad under adult supervision.
- ensure that their iPad is kept in their bag before 8:50am and after 3:00pm and is not used during these times.
- exercise responsible behaviour when using the iPad.
- respect the copyright of the images and other media that are accessed.
- use recommended personal headphones with their iPad.
- **connect to Apple Classroom** in all classes in which they use their iPad.
- honour this 1:1 iPad iPromise.

Parents will:

- be responsible for maintaining the iPad.
- be aware of how their child is using the iPad at home.
- talk to their children about how to use the internet safely and effectively.
- support the school in their delivery of consequences for inappropriate use of the iPad at school.
- update and install apps as required.
- be responsible for insuring their child's iPad (School insurance will not cover personal student iPads).
- contact their insurance company if the iPad is damaged or stolen at school.
- be responsible for any damage or loss of their child's iPad.

Online Services Users *will NOT*:

- access apps which are not relevant to education/ classroom topics.
- play games using the iPad (unless under the teacher's instruction).
- allow other students to use their personal iPad.

What Happens if the 1:1 iPad iPromise is Broken?

- loss of iPad privileges for a length of time determined by the teacher and school leadership.
- parents will be informed about the breach.
- parents will meet with the classroom teachers and/or member of the leadership team to discuss the breach and consequences thereof.