

**eSmart**

**Policy**

# Wandin North Primary School

**eSmart Policy**

**RATIONALE:**

The School aims to provide an eSmart culture within the educative environment which is in keeping with the values of the School, legislative and professional obligations, and the community’s expectation. Within this context, the objective of this Policy is to ensure the smart, safe, responsible use of ICT within the school community. This Policy outlines the conditions applying to the use of all school ICT and behaviours associated with safe, responsible and ethical use of technology. Users are required to comply with the eSmart Policy. The eSmart Policy is supported by:

* ICT Policy
* iPad Policy & User Agreement
* Social Media Policy
* Student Internet and Email Agreement (Years 1-6)
* Internet and Network User Agreement (Prep)

**BREACH OF AGREEMENT:**

Breaches of this Agreement can undermine the values of the school and the safety of the eLearning environment, especially when ICT is used to facilitate misconduct. Such a breach which is deemed by the school to be harmful to the safety of the school may possibly result in serious disciplinary action such as:

* Withdrawal of access to the school network and devices
* Confiscation of personal devices used inappropriately throughout the school day, including all excursions and camps.
* Devices believed to contain evidence of a criminal act may be held and handed to Police for evidence in line with Police timelines
* Confiscated devices used inappropriately (not required for evidence of a criminal act) can be collected by the student or parent as determined by the Principal’s nominee at the end of the day
* Suspension in cases of serious misconduct
* It is a criminal offence to use an ICT device to menace, harass, make threats, or offend another person. In these instances, the school may consider it appropriate to involve police.

In investigating a suspected breach of this Policy the User agrees to promptly make the ICT equipment/device available to the school for the purpose of any investigation and/or audit and to cooperate otherwise with the school in any investigation or audit process. The terms of this Policy form part of the school’s expectations for the purposes of a student’s enrolment at the school.

**USER eSMART OBLIGATIONS**

**1. Authorised Usage and eSmart Agreement**

1.1. As the school provides network access, the contents of the school ICT system remain the property of the school. The school has the capacity to monitor and control the system and reserves the right to monitor individual usage and report, where necessary, any indications of misconduct or prohibited use.

1.2. All users, whether or not they make use of network facilities and communication technologies on school owned or personal ICT equipment/devices will have full access to this policy via the school web page

1.3. The school’s ICT, including network facilities, communication technologies, eLearning tools and ICT equipment/devices all fall under this policy. The use of personal ICT and communication devices fall under this policy when used for the purpose of communicating about school community members.

1.4. The school encourages anyone with a query about the eSmart Policy to contact the school on 5964 4570.

**2. Obligations and requirements regarding appropriate use of ICT in the school learning environment**

2.1. While on campus, using school owned or personal ICT equipment/devices, including mobile phones, is for educational purposes only.

2.2. When using school or privately owned ICT on the school site or at any school related activity prohibited use includes, ***but is not limited to***, any conduct that is defined as objectionable and inappropriate:

* Would cause offense to students, teachers or parents, such as profanity, offensive language, obscenity, pornography, unethical or illegal solicitation, racism, sexism
* Is derogatory or threatening to another e.g. libellous, slanderous, inflammatory, threatening, harassing
* Has intention to deceive, impersonate or misrepresent
* Forwards confidential messages to persons to whom transmission was never authorised by the school, including persons within the school community and persons/organisations outside the school community
* Fails to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus
* Breaches copyright
* Attempts to breach security and infrastructure that is in place to protect user safety and privacy
* Brings the school into ill repute
* Results in unauthorised external administration access to the school’s electronic communication
* Propagates chain emails or uses groups or lists inappropriately to disseminate information
* Inhibits the user’s ability to perform their duties productively and without unnecessary interruption
* Interferes with the ability of others to conduct the business of the school
* Involves malicious activity resulting in deliberate damage to school ICT and/or ICT equipment/devices.
* Involves the unauthorised installation and/or downloading of non-school endorsed software
* Breaches the ethos and values of the school

2.3. In the event of accidental access of such material, Authorised Users must:

* Not show others
* Close or minimise the window
* Report the incident immediately to the supervising teacher or classroom learning assistant.

2.4. A person who encourages, participates or otherwise knowingly acquiesces in prohibited use of school, or privately owned communication technologies, on the school site or at any school related activity, may also be found to have engaged in prohibited use

2.5. While at the school or a school related activity, Users must not have involvement with any material which might place them at risk or breaches the ethos of the eSmart Policy. This includes images or material stored on privately owned ICT equipment/devices brought onto the school site, or to any school related activity such as USB sticks.

2.6. Users must not attempt to download, install or connect any unauthorised software or hardware onto school ICT equipment, or utilise such software/hardware. This includes use of such technologies as Bluetooth, infrared, and wireless, and any other similar technologies that are available. Any Users with a query or a concern about that issue must speak with their classroom teacher.

**3. Monitoring by the School**

The school:

3.1. Reserves the right at any time to check work or data on the school’s computer network, email, internet, computers and other school ICT equipment/devices, without obtaining prior consent from the relevant User.

3.2. Reserves the right at any time to check work or data on privately owned ICT equipment on the school site or at any school related activity. The User agrees to promptly make the ICT equipment/device available to the school for purposes of any such check and to otherwise co-operate with the school in the process. Before commencing the check, the school will inform the User of the purpose of the check.

3.3. Monitors traffic and material sent and received using the school’s ICT infrastructures. From time to time this may be analysed and monitored to help maintain an eSmart learning environment.

3.4. From time to time conduct an internal audit of its computer network, internet access facilities, computers and other school ICT equipment/devices, or may commission an independent audit of content and usage.

**4. Copyright, Licensing, and Publication**

4.1. Copyright laws and licensing agreements must be respected and sources appropriately acknowledged. Users must not breach laws of copyright, moral right or intellectual property – this includes illegal copies of software, music, videos, images.

4.2. All material submitted for internal publication must be appropriate to the school environment and copyright laws.

**5. Individual password logons to user accounts**

5.1. If access is required to the school computer network, computers, and internet access using school facilities, it is necessary to obtain a personal user account from the school.

5.2. Users must keep usernames and passwords confidential and not share them with anyone else. A breach of this rule could lead to users being denied access to the system.

5.3. Authorised users must not allow another person access to any equipment/device logged in under their own user account. Material accessed on a user account is the responsibility of that user. Any inappropriate or illegal use of the computer facilities and other school ICT equipment/devices can be traced by means of this login information.

5.4. Those provided with individual, class or group email accounts must use them in a responsible manner and in accordance with the Policy. This includes ensuring that no electronic communications could cause offence to others or harass or harm them, put the owner of the user account at potential risk, contain objectionable material or in any other way be inappropriate in the school environment.

5.5. For personal safety and having regard to Privacy laws, Authorised Users must not reveal personal information about themselves or others. Personal information may include, but is not limited to, home or email addresses, and any telephone numbers, including mobile numbers.

**6. Other User obligations**

6.1. Avoid deliberate wastage of ICT related resources including bandwidth, through actions such as unnecessary printing and unnecessary internet access, uploads or downloads.

6.2. Avoid involvement in any incident in which ICT is used to send or display electronic communication, graphics, audio, video files which might cause offence to others and/or involve objectionable material.

6.3. Abide by copyright laws and obtain permission from any individual before photographing, videoing or recording them.

6.4. Not upload, to a publicly accessible platform, any image or video taken at the school or of any student in school uniform without the written consent of parents/guardians and the Principal.

**7. Privacy**

7.1. The Privacy Act requires the school to take reasonable steps to protect the personal information that is held by the school from misuse and unauthorised access. Users must take responsibility for the security of their computer and not allow it to be used by unauthorised persons.

7.2. While **after school use** of communication technologies by students is the responsibility of parents, school policy requires that no student attending the school may identify, discuss, photograph or otherwise publish personal information or personal opinions about school staff, fellow students or the school. Any such behaviour that impacts negatively on the high public standing of the school may result in disciplinary action. The school takes a strong position to protect privacy and prevent personal information and opinion being published over technology networks including Facebook, Twitter, the School Website, YouTube and any further new technology.

**8. Procedures for Mobile Phone and Personal Device Use at School**

Wandin North Primary School accepts that parents provide their children with mobile phones and other personal devices in order that their child may communicate with them in the event of an emergency. Mobile phones and other personal devices are often provided for the use of children travelling alone on public transport or commuting to school. It is acknowledged that providing a child with a mobile phone or other personal device gives parents reassurance that they can speak with their child quickly, at any time.

However, while at school, using school owned or personal ICT equipment/devices, including mobile phones, is for educational purposes only and parents who need to contact their child during school hours should do so by placing a call to school Administration. Mobile phones and other personal devices are to be left at school Administration for safe keeping during school hours.

**Responsibility**

8.1. It is the responsibility of students who bring mobile phones and other personal devices onto school premises to adhere to the guidelines outlined in this document.

8.2. The decision to provide a mobile phone and other personal device to their children should be made by parents or guardians.

8.3. Parents should be aware if their child takes a mobile phone or other personal device onto school premises.

8.4. Mobile phones and other personal devices which are found in the school and whose owner cannot be located are to be handed to school Administration.

8.5. The school accepts no responsibility for replacing lost, stolen or damaged mobile phones and other personal devices. Their safety and security is wholly in the hands of the student.

8.6. The school accepts no responsibility for students who lose or have their mobile phones and other personal devices stolen while travelling to and from school.

8.7. It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones (e.g. by other students, or if stolen). Students must keep their password/pin numbers confidential. Mobile phones and other personal devices and/or passwords may not be shared.

8.8. Students protect the privacy and dignity of individuals and security of information, to maintain the high public standing of St Paul’s School and compliance with State and Federal laws.

8.10. The school strongly advises that for safety reasons headphones are not used when students are travelling to and from school, eg. walking, riding a bike, moving on and off buses.

8.11. Any mobile phone and other personal device being used during the school day will be confiscated. Parents are reminded that in cases of emergency, the school’s Administration remains a vital and appropriate point of contact and can ensure your child is reached quickly, and assisted in the appropriate way.

**9. When using a digital device such as a camera or iPad students will:**

9.1 Only take photos and record sound or video with the permission of the teacher when it is part of a class or lesson.

9.2 Seek permission from individuals involved before taking photos, recording sound or videoing them (including teaching staff).

9.3 Seek appropriate (written) permission from individuals involved before publishing or sending photos, recorded sound or video to anyone else or to any online space.

9.4 Seek written permission from the principal before uploading any image, sound or recording taken at Wandin North Primary School, or any image of anyone in Wandin North Primary School uniform, to a *publicly accessible platform*.

9.5 Students, parents and staff should be respectful in photos taken or video captured and never use these as a tool for bullying or harassment.

**How else can parents/carers assist?**

* Reinforce the eSmart policy with your child
* Encourage your child to comply with the school’s eSmart policy
* Support the school in the enforcement of the eSmart policy
* Not attempt to call your child’s mobile phone during school hours. Contact the school directly on 5964 4570 if you need to get an urgent message to your child.

**REVIEW:**

* The School Advisory Board and staff regularly monitor and review the effectiveness of the eSmart policy as past of the school’s three year cycle and revise the policy when required.

February 2017

This policy was last endorsed by the School Advisory Board on…