Pennant Hills Public School

Bring Your Own Device

Policy

PENNANT HILLS PUBLIC SCHOOL
STUDENT BRING YOUR OWN DEVICE (BYOD) POLICY

1. Introduction

BYOD (Bring Your Own Device) is a strategy that is governed by the NSW Department of Education's (DoE) *Student Bring Your Own Device (BYOD) Guidelines* which enables students to bring their own device to the classroom if they wish to do so. Student participation in BYOD is optional and all students will be able to engage fully in classroom activities.

The term "device" in this policy refers to personal mobile electronic devices, including assistive technologies, brought into the school, which is owned by the student, and which has the capability of connecting to the department's Wi-Fi network. Mobile phones are not part of the school's program and will not be able to be connected to the department's wireless network.

This document provides information and advice to parents, students and teachers as we collectively explore and learn together through the Pennant Hills Public School's BYOD (Bring Your Own Device) program. As part of this, our Frequently Asked Questions (FAQ's) on the school website will be updated on this journey together.

2. Purpose

As we enter a new era of education with the new National Curriculum, schools are challenged to assist students in engaging and energetic ways to develop their 21st Century learning skills. At Pennant Hills Public School, based on the Department of Education's current educational research, mobile devices present as a relevant, known and effective learning tool that help facilitate the development of 21st Century learning skills within our primary school classrooms.

A mobile device for your child will further support their learning, will provide your child with the opportunity for anywhere/anytime learning, and will expand the learning opportunities for our students.

Importantly, it will be used in the context of regular lessons and teacher programs and in accordance with the school meeting its obligations in terms of all existing Board of Studies Teaching and Educational Standards (BOSTES) syllabus documents.

3. Key Considerations

Some of our key considerations in working with our community to implement BYOD are:

3.1 The widespread availability of wireless internet-enabled devices.

3.2 The integral nature of these devices to the students' own world.

3.3 The possibility of leveraging students' attachment to their own devices to deepen learning and to make learning more personalised and student-centred.

4. Policy Requirements

4.1 Students bring devices to school for the purpose of learning. In allowing students to bring devices to school for the purpose of learning, recreational gaming is not permitted.

4.2 Use of devices at school will be governed by this policy which has been shaped by community consultation.

4.3 Information, links and Frequently Asked Questions are available on our school website at www.pennanthil-p.schools.nsw.edu.au

4.4 Students and their parents/caregivers must complete and return a signed BYOD Student Agreement prior to participation in BYOD.

4.5 The school has strategies and resources to ensure that all students are able to engage fully in classroom activities. Students without a device will be accommodated.

5. Access to the Department's Wi-Fi network and resources

5.1 Internet access through the department's Wi-Fi network will be provided on departmental sites at no cost to students who are enrolled in NSW public schools.

5.2 Students are encouraged to save and back up all work on their hard drives and cloud accounts as access to share drives and printers is limited.

6. Acceptable use of devices

The principal will retain the right to determine what is, and is not, appropriate use of devices at the school within the bounds of the department's policies and NSW privacy and other legislation.

The following is derived directly from the NSW Department of Education's (DoE) Student Bring Your Own Device (BYOD) Guidelines.

6.1 Students must comply with departmental and school policies concerning the use of devices at school while connected to the department's Wi-Fi network.

6.2 Use of personal devices during the school day is at the discretion of teachers. Students must only use their devices as directed by their teacher.

6.3 Mobile phones and mobile network enabled devices are not part of PHPS's BYOD program.

6.4 Mobile phone voice and text, SMS messaging or device instant messaging use by students during school hours is not permitted.

6.5 Students should not attach any school-owned equipment to their mobile devices without the permission of their teacher.

6.6 Students must not create, transmit, retransmit or participate in the circulation of content on their devices that attempts to undermine, hack or bypass any hardware and software security mechanisms that have been implemented by the department, its Information Technology Directorate or the school.

6.7 Students must not copy, transmit or retransmit any material that is protected by copyright, without prior permission from the copyright owner.

6.8 Students must not take photos or make video or audio recordings of any individual or group without the express written permission of each individual (including parent/caregiver consent for minors) being recorded and the permission of an appropriate staff member.

6.9 Students must not use the department's network services to seek out, access, store or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature is prohibited. Such use may result in disciplinary and/or legal action.

6.10 Students and their parents/caregivers must be advised that activity on the internet is recorded and that these records may be used in investigations, court proceedings or for other legal reasons.

6.11 Personal content on personal devices is not to be shared.

6.12 Students should not use another student's personal device. Teaching and learning materials may be shared between students.

6.13 Students shall comply with departmental or school policies concerning the use of personal devices at school and while connected to the DoE's network including:
Online Communication Services – Acceptable Usage for School Students

Where a school has reasonable grounds to suspect that a device contains data which breaches the BYOD Student Agreement, the principal may confiscate the device for the purpose of confirming the existence of the material. Depending on the

nature of the material involved, school disciplinary action may be appropriate or further action may be taken including referral to the police.
The consequences of any breaches of the school's BYOD policy will be determined by the principal in accordance with relevant Department policies and procedures and accepted school practice.

7. BYOD Student Agreement

Prior to connecting their devices to the department's Wi-Fi network, students must return a BYOD Student Agreement.

7.1 The BYOD Student/Parent Agreement contains both BYOD Device Requirements and BYOD Student Responsibilities.

7.2 All sections of the BYOD Student/Parent Agreement must be ticked and signed by the student and by a parent/caregiver.

7.3 By accepting the terms of the BYOD Student Agreement, the student and parents/caregivers acknowledge that the student:

- agrees to comply with the conditions of the school's BYOD policy;
- and understands that noncompliance may result in disciplinary action.

Schools should retain a copy of the BYOD Student Agreement in print or electronic form and it will be kept on file with the student record.

8. Long-term care and support of devices

Students and their parents/caregivers are solely responsible for the care and maintenance of their devices.

8.1 Students must have a supported operating system and current antivirus software, if applicable, installed on their device and must continue to maintain the latest service packs, updates and antivirus definitions as outlined on the BYOD Student Responsibilities document.

8.2 Students are responsible for ensuring the operating system and all software on their device is legally and appropriately licensed.

8.3 Students are responsible for managing the battery life of their device. Students should ensure that their devices are fully charged before bringing them to school. Schools are not responsible for (or restricted from) providing facilities for students to charge their devices.

8.4 Students are responsible for securing and protecting their device in school, and while travelling to and from school. This includes protective/carry cases and exercising common sense when storing the device.

8.5 Students should clearly label their device for identification purposes. Labels should not be easily removable.

8.6 Students should understand the limitations of the manufacturer's warranty on their devices, both in duration and in coverage.

9. Damage and loss

9.1 Students bring their devices on to the school site at their own risk.

9.2 In cases of malicious damage or theft of another student's device, existing school processes for damage to the school's or another student's property apply.

10. Technical Support

The school will provide as much technical support as possible to assist students in participating in lessons. The school will continue to invest in fortnightly support provided by an external technician. In the event of a device not responding, basic support will be provided and/or a school device provided, as required. Parents will be contacted to discuss any ongoing issues with the device. The Department of Education's Information Technology Directorate offers technology support for its schools and their internal technology networks.

11. Insurance

Students' personal devices are not covered by Treasury Managed Fund. Insurance is the responsibility of parents/ caregivers and students.

When parents/carers purchase their child's device, they may also purchase an optional insurance policy from the supplier of their device or a relevant insurance company. As mobile devices are subject to a higher risk of accidental damage, prior to signing up for an insurance policy, parents should be fully aware of the details and limitations of the policy, including any excess charged for making a claim, and the name of the company that holds the policy. As a guide, a suitable BYOD insurance policy should cover all types of BYODs and provide worldwide replacement cost coverage against things such as:

- Accidental damage
- Damage from falls and liquids
- Theft
- Fire
- Vandalism
- Natural disasters (such as floods, cyclones, earthquakes, tornadoes, water damage, and power surge due to lightning).

12. DEC technology standards

The department's Wi-Fi network installed in primary schools operates on the 802.11n 5Ghz standard. Devices that do not support this standard will not be able to connect.

13. Device requirements

The BYOD Minimum Specification Device Requirements' document and the BYOD Student Parent agreement document includes information on:

- Departmental technology standards
- Hardware specifications, including the operating system
- Software and apps
- Battery life/spare batteries/battery charging
- Protective casing (scratch/impact/liquid-splash resistant)
- Device insurance/safety
- Ergonomics (keyboard, stand)
- Back-up storage such as Google drive.

14. Security and device management processes

Students using personal devices at PHPS should consider the following:

- Strong passwords (your portal has password help information, as well as this issue being covered regularly in digital citizenship lessons)
- Device anti-virus software
- Privacy controls (not sharing passwords)
- Internet filtering (at school this is provided by the DoE)
- Student digital citizenship and cyber safety
- Report any content that may be considered offensive/inappropriate or dangerous **immediately** to a teacher/parent/carer.

All activity conducted through the DoE Wi-Fi network is logged and can be traced to users.

The department's Digital Citizenship (www.digitalcitizenship.nsw.edu.au) website contains information to support security and device management.

15. Teacher/School Responsibilities

15.1 Teachers should encourage and facilitate the use of students' devices in their classes as required and as appropriate. Delivery of all elements of the BOSTES syllabus documents occurs simultaneously. Significantly, BYOD does not mean other skills, practices and learning does not occur.

15.2 Use of students' own devices in class is necessarily at the discretion of the teacher.

15.3 Teachers will incorporate digital citizenship lessons including cyber-safety and device management lessons in the context of their teaching and learning activities.

15.4 Teachers will secure classrooms containing devices during breaks or when the room is unattended.

15.5 Teachers will secure a student's device overnight if they are aware it has been left at school accidentally.

15.6 Teachers will maintain telephone or written communication with parents in regards to device management, where required.

15.7 Teachers will provide minimal technical support to the best of their abilities when required – and seek further assistance at the end of a school day if a more complex issue arises.

16. Student/ Parent Responsibilities

Students and parents are responsible for the care and maintenance of their personal devices. This includes but is not limited to:

16.1 Managing battery life and regular charging of their device at home.

16.2 Labelling their device and providing the device serial number to the school for identification purposes.

16.3 Providing and using device protective casing.

16.4 Ensuring the device is safe and secure during travel to and from school and throughout the school day.

16.5 Placing the device in the provided receptacle on arrival at school after the morning bell.

16.6 Maintaining up-to-date anti-virus software and operating systems on their device and ensuring all software is legally and appropriately licenced.

16.7 Removing SIM Card and storing it at home. The use of 3G and 4G wireless connections is not permitted.

16.8 Taking insurance coverage of their own device to protect any accidental damage, theft or loss.

16.9 Deactivating, by signing out of, instant messaging, texting, Apple ID /Windows ID, FaceTime or any other applications that are linked to parents'/carer's credit card details.

17. Equity of access to technology

The school acknowledges the difficulties that some families have in providing technology for learning for their children. PHPS will maintain devices, to ensure equity of access. Should a personal device be unexpectedly unavailable for a short time, students will be provided access to a school device.

- Regrettably, the school cannot loan or assign a device or make a device available for a permanent or semi-permanent loan.

- In substitution of a personally owned device the school will consider options for students including:
    - Priority or reserved access to desktop computers, computer labs within classrooms or the library during class time, before school or during breaks.
    - Loan of a laptop or other device for a particular period or class.
    - Loan of a laptop or other device for a particular day.
    - Recurrent daily loan of a laptop or other device.

18. Education Software

All NSW Department of Education school students are eligible to download and licence Adobe and Microsoft software from their portal. This software is only available to download onto personally owned devices.

- Students will need to use their @education.nsw.gov.au student email address to register on their first visit.
- To register, click on the “Sign In” link at the top of the page and then click on the REGISTER button. A verification email will be sent to their DoE email address. To complete the registration please select the link provided in the email.
- *Note: Individual students are eligible for one download per application only.*