PIMLICO STATE HIGH SCHOOL
Making a world of difference

BYOD Student Charter

Table of Contents

OVERVIEW

Over the past decade, technology, as well as the expectations of our students, have significantly changed. These have impacted on what we teach and how students learn. It is therefore important that schools provide opportunities for students to develop the knowledge, skills and attitudes that will prepare them for a future in the 21st century. For students, having access to a digital device at home and at school, enables them to extend their learning beyond the classroom.

To assist this process, Pimlico State High School operates a Bring Your Own Device (BYOD) program. The goal is to enable every student the opportunity to be effective digital learners, who become confident, creative and productive in the digital world.

WHAT IS BYOD?

The BYOD program allows students to bring their own personal computing device to school, for the purposes of assisting them with their learning. Students will be able to connect their private device to the school's wireless network in order to access:

- home directory on the school network
- Curriculum Drive (where teachers store digital resources)
- school email services
- filtered internet services

Access to the school's computer network is only provided if the mobile device meets the Department of Education and Training's technical and security requirements.

STUDENT INVOLVEMENT IN PROGRAM

The BYOD program is open to all Pimlico State High School students (Year 7 through to Year 12).

Parents wishing their child to participate in the BYOD Program should read and understand the details included in this document, as well as associated policies indicated.

WHAT IS REQUIRED TO PARTICIPATE IN THE PROGRAM?

In Years 7 and 10-12 at Pimlico State High School, it is a requirement that all students bring their own computer device to school, each day. The preferred device is a Windows 2-in-1 tablet, although an updated Windows laptop or Apple MacBook is also acceptable.

All new Windows 11 laptop devices purchased from a major electronics retailer will be compatible. All new MacBooks can be supported, but will add complexity for students connecting to the network.

Chromebooks, Android tablets, iPads and other laptop devices that are not running at least Windows 10 or macOS13 are not compatible in any capacity due to limitations of the current parameters of the BYOD program controlled by the Department of Education.

GUIDELINES FOR PURCHASING A DEVICE

Our recommended device is a new Windows 11, 2-in-1 device + stylus. Students with such devices have reported greater satisfaction with the BYOD program.

Ensure all devices are kept current with Windows and macOS updates to ensure BYOD connectivity. Parental controls and limited user accounts will prevent initial BYOD connectivity, but can be reenabled once students have connected to the school network.

We continue to recommend that parents do not purchase additional third-party software. The free Windows Defender continues to provide the best antivirus protection for students' usage. Office 365 is available for free to all EQ students through the Microsoft website.

For second-hand or clearance devices running Windows 10, the minimum specifications are:

Component:	Minimum Specifications
Processor:	Intel CORE iSeries or AMD Ryzen CPU
RAM:	8gb of RAM
Storage:	128gb SSD
WiFi:	Dual-band WiFi: sometimes marketed as WiFi802.11ax or WiFi6
Battery:	Battery must provide at least 6 hours of continuous operation

NOTE: Some subject areas recommend a higher processor and RAM due to the software being used. These subjects include Design, and Film, Television and New Media.

Any device brought into the school, should be clearly labelled with the student's name.
When purchasing a new device, parents should consider the following questions:

1. How long will the device be expected to be used by the student?

Many users would expect a laptop to be replaced within three years. If this was the case, an entry level laptop may be appropriate for a student enrolled in Year 7, while in Year 10 a device with a higher hardware specification would be desirable. Another factor to consider is that technology changes quickly. A device that meets your student's current needs, purchased at a relatively inexpensive price, may be easier to replace in the future, compared to a laptop that is more expensive. Also consider that if damage was to occur to the device, it is likely to cost more to replace parts damaged on an expensive model, compared to a cheaper device. If a screen was broken on a cheaper model, it may be more economical to purchase a new device, rather than repair the damage.

2. What will happen if repairs need to be completed?

There is a significant advantage if repairs to the laptop can be completed locally, as this usually reduces the time delay in having the device returned to the student. There is a further advantage if repairs can be completed at your home, rather than having to send the device away.

3. What warranty is provided, how long and what exactly does it cover?

The school would strongly encourage that you purchase a warranty that will last the same number of years that you expect your child to be using the laptop. Make sure you know what exactly will be covered (parts/labour), where the repairs will occur and what additional cost may be incurred by you.

The school also encourages internet filtering software be purchased and installed on the device, to ensure that the student does not access inappropriate web sites at home. While at school, filtered internet access will be provided.

SOFTWARE

Free - Microsoft Office 365

All Queensland state school students can download a copy of the latest Microsoft Office 365 to their personal home computers and mobile devices. Using your student's @eq.edu.au email address and login, navigate to https://portal.office.com/ols/mysoftware.aspx and follow the prompts to download and execute OfficeSetup.exe.

Web Browser

Windows devices come with Microsoft Edge installed by default. Microsoft Edge is the preferred browser due to its accessibility and annotations functions, which are used in class learning. Keeping this software up-to-date will allow students to access all of the school's online resources.

Anti-virus software

The school strongly encourages that all Windows devices use Windows Defender program functioning correctly and updated regularly. Commercial anti-virus software may be used, but may cause conflicts with required subject software. Apple devices should use reputable, commercial anti-virus software.

Subject Software

Due to licencing conditions, school owned software cannot be installed on private devices. Some subjects may require students to download software from the internet. These programs are usually free, however will require an internet connection to download.

Note that the installation and maintenance of software on a student's personal device, is the responsibility of the student and their family.

CARE AND USE OF DEVICE

Carry Case

It is highly recommended that a carry case be purchased for the student's device. The case should be strong, sturdy and at least water resistant. The case should be clearly labelled with the student's name. Students should also carry a zip lock resealable plastic bag, so that the device can be protected in case of heavy rain.

Printing

BYOD printing to Library printers is available through the BYOx Mapper app used to enrol in BYOD.

Charging Of Device (Battery Power)

Students will usually not be able to charge their device during class due to the limited availability of power outlets. The device used should have sufficient battery power to last an entire day. When charging the device at home, the correct power adapter should be used, otherwise damage to the device may occur. Safety procedures should always be considered when charging electrical devices.

Use of Wi-Fi

Connection of private devices to the school's computer network will be via the school's wi-fi network. The steps to complete this process can be found at the back of this document.

Backing up Data

Technology can fail, can be lost or stolen. It is extremely important that students have a backup plan in case things go wrong. The school network drives are backed up daily and represent the most secure option for storing school work.

For work taken between home and school, students are encouraged to copy their most important files to an external hard drive or USB memory stick. An additional strategy to assist in ensuring a backup copy of a document exists, is to email themselves a copy of the document.

Security of Device

Devices are the sole responsibility of the family. The school accepts no responsibility for the security or safety of the device. Teachers and staff will not store or look after a device on behalf of students.

Should damage to the device occur whilst at school by another student/s, the school is not at liberty to provide parents with details about other students or provide contact details of the parents of students who may have been involved in the incident.

Pimlico State High School does not accept responsibility for damage, loss or theft of the BYOD device.

Accidental Damage, Theft and Insurance
It is highly advisable that parents purchase Accidental Damage Protection for their child's BYOD device. Accidental Damage Insurance should cover the device for accidental damage on and off the school campus. Repairing a cracked screen can cost more than $400.00, depending on the model of the device and labour costs involved.

To cover for theft, fire and other issues, the school also recommends that the device be included in your family's Home and Contents Insurance Policy. There may be a requirement by your Insurance Company to individually list the device on your insurance policy.

Insurance can often be purchased from the computer vendor or your existing insurance company. All insurance claims are to be settled between the family and the insurance company. The school will not be involved in any insurance claims or disputes.

Repairs and Maintenance
It is the responsibility of families to keep their student's device in good working order, to ensure minimal disruption to student learning. All maintenance for the device, operating system, software and apps purchased, are the responsibility of the family. It is expected that students bring their device to school each day, fully charged.

When moving from class to class, students should take care to put their device to sleep. Failure to do so can damage the hard drive of the device and potentially corrupt files. Choosing a device with a solid state drive (SDD), can alleviate some of these issues, but increases the cost of purchasing the device.

A limited number of loan devices are available to students that bring proof that their regular device is unavailable for repairs. Additional information, and access to the loan devices is available through the school's website.

WEB FILTERING

The internet has become a powerful tool for teaching and learning, however students need to be careful and vigilant regarding some web content. At all times while using ICT resources, students will be required to act in accordance with the requirements of the Code of School Behaviour. To help protect students (and staff) from malicious web activity and inappropriate websites, the Department of Education, operates a comprehensive web filtering system. Any device connected to the internet through the school's computer network will have filtering applied.

The filtering system provides a layer of protection to staff and students against:
- inappropriate web pages
- spyware and malware
- peer-to-peer sessions
- scams and identity theft

This purpose-built web filtering solution takes a precautionary approach to blocking web sites, including those that do not disclose information about their purpose and content. The Queensland Department of Education's filtering approach represents global best practice in internet protection measures. However, despite internal departmental controls to manage content accessed from the internet, illegal, dangerous or offensive information may be accessed or accidentally displayed. Teachers will always exercise their duty of care, but avoiding or reducing access to harmful information also requires responsible use by the student.

Students are required to report any internet site accessed that is considered inappropriate. Any suspected security breach involving students, users from other schools or from outside the Queensland Department of Education network, must also be reported to the school.

Personally owned devices have access to home and other out of school internet services and those services may not include any internet filtering. Parents and caregivers are encouraged to install a local filtering application on the student's device for when they are connected in locations other than school. Parents / caregivers are responsible for the appropriate internet use by students outside the school.

Current technology allows laptop devices to connect to mobile phones, in order to access email and internet services. The phone becomes a 'hot spot' for the student to access internet services. The school strongly discourages this practice, as accessing the internet without adequate filtering software installed, is likely to result in the student accessing inappropriate material.

CYBERSAFETY

If a student believes they have received a computer virus, spam, or they have received a message or other online content that is inappropriate or makes them feel uncomfortable, they should inform their teacher, parent or caregiver as soon as possible. Students should also seek advice if another user seeks personal information, asks to be contacted by phone, offers gifts by email or asks to meet a student.

Students must never initiate or knowingly forward emails or other online content, containing

- a message sent to them in confidence
- a computer virus or attachment that is capable of damaging the recipients' computer
- chain letters or hoax emails
- spam (such as unsolicited advertising)

Students must never send, post or publish:

- inappropriate or unlawful content which is offensive, abusive or discriminatory
- threats, bullying or harassment of another person
- sexually explicit or sexually suggestive content or correspondence
- false or defamatory information about a person or organisation

Parents, carers and students are encouraged to read information available at the Office of the Children's eSafety Commissioner (https://esafety.gov.au).

ACCEPTABLE USE OF TECHNOLOGY

Upon enrolment in a Queensland Government school, parental or caregiver permission is required in order to give a student access to the department's technology and internet resources. Parents/carers and students are required to read and sign the Acceptable Use of the Department's Information, Communication and Technology (ICT) Networks and Systems.

This policy also forms part of the BYOD Student Charter. The acceptable use conditions apply to the use of the student's personal mobile device and use of the internet, while on school grounds.

Examples of responsible use of devices for students include:

- engagement in class work and assignments
- developing appropriate 21st Century knowledge, skills and behaviours
- authoring text, artwork, audio and visual material for publication on the school intranet or internet, for educational purposes, as supervised by school staff
- conducting general research for school activities and projects
- communicating or collaborating with other students, teachers, parents, caregivers or experts, as part of assigned school work
- accessing online references such as dictionaries and encyclopaedias
- using the department's eLearning Courses
- ensuring that the device is fully charged before bringing it to school

While connected to the school computer network, students should not:

- create, participate in or circulate content that attempts to undermine, access into and/or bypass the hardware and/or software security mechanisms that are in place
- authoring text, artwork, audio and visual material for publication on the school intranet or internet, for educational purposes, as supervised by school staff
- conducting general research for school activities and projects
- communicating or collaborating with other students, teachers, parents, caregivers or experts, as part of assigned school work
- accessing online references such as dictionaries and encyclopaedias
- using the department's eLearning Courses
- ensuring that the device is fully charged before bringing it to school

While connected to the school computer network, students should not:

- create, participate in or circulate content that attempts to undermine, access into and/or bypass the hardware and/or software security mechanisms that are in place
- disable settings for virus protection, spam (unsolicited email) and/or internet filtering that have been applied as part of the department's security protocols
- use unauthorised programs and intentionally download unauthorised software, graphics or music
- intentionally damage or disable computers, computer systems, school or government networks
- use the device for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose

Students' use of the internet and online communication services, may be audited at the request of appropriate authorities for investigative purposes surrounding inappropriate use.

Information sent or recorded by a student's personal mobile device, contributes to the community perception of the school. All students using ICT resources are expected to conduct themselves as positive ambassadors for the school. Students must not record, photograph or film any students or school personnel without the express permission of the individual/s concerned.

PRIVACY AND CONFIDENTIALITY

Students must not use another student or staff member's username or password to access the school network or another student's device, including not trespassing in another person's files, home drive, email or accessing unauthorised network drives or systems.

Additionally, students should not divulge personal information via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school. It is important that students do not publish or disclose the email address of a staff member or student, without that person's explicit permission. Students should also not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. They should ensure that privacy and confidentiality is always maintained.

INTELLECTUAL PROPERTY AND COPYRIGHT

Students should never plagiarise information and should observe appropriate copyright clearance, including acknowledging the original author or source of any information, images, audio or resources used. It is also important that the student obtain all appropriate permissions before electronically publishing other people's works or drawings. The creator or author of any material published should always be acknowledged. Material being published on the internet or school intranet must have the approval of the principal or their delegate and have appropriate copyright clearance.

Copying of software, information, graphics or other data files may violate copyright laws and individuals may be subject to prosecution from agencies to enforce such copyrights.

MONITORING AND REPORTING

Students should be aware that the use of internet and online communication services can be audited and traced to the account of the user. All material on a personal device is subject to audit by authorised school staff. If at any stage there is a police request, the school may be required to provide the authorities with access to the device and personal belongings associated with its use.

MISUSE AND BREACHES OF ACCEPTABLE USAGE

Students should be aware that they are held responsible for their actions while using their device and accessing the internet and online communication services. Students will be held responsible for any breaches caused by other person(s) knowingly using their account to access internet and online communication services.

The school reserves the right to restrict or remove access of personally owned mobile devices from accessing the intranet, internet, email or other network facilities. This is to ensure the integrity and security of the network and to provide a safe working and learning environment for all network users. The misuse of personally owned mobile devices may result in disciplinary action that includes, but is not limited to, the withdrawal of access to school technology services.

In certain circumstances, the school may temporarily confiscate the student's device in relation to our Use of mobile phones and other devices by students Policy in our Student Code of Conduct. Unlawful or suspected unlawful use of the device at school will result in the device being confiscated and handed to the Queensland Police Service for further investigation.

SCHOOL TECHNICAL SUPPORT

As indicated, all issues surrounding software and maintenance of the device is the responsibility of the student and their family. The school will only be providing technical support to assist a student connecting to the school computer network (if required). Support can be obtained by emailing: itsupport@pimlicoshs.eq.edu.au

PARTICIPATION COST

Costs associated with access to the school's network are already incorporated into the school's student resource scheme levy. There is no additional cost for participating in this program.

RESPONSIBLE USE OF BYOD DEVICE

Our goal is to ensure the safe and responsible use of facilities, services and resources available through the provision of clear guidelines.

Responsibility of Stakeholders involved in the BYOD Program

School

- Provide information and guidelines on the BYOD Program
- Provide network connection (provision of network hardware and licence requirements)
- Provide Internet filtering
- Provide email access

Student

- Acknowledge that the purpose of using the device at school is to assist the student with their school studies
- Care for the device and ensure that it is secure at all times
- Display appropriate digital citizenship and online safety awareness
- Use passwords that provide a level of difficulty so that others cannot simply guess the password
- Passwords are to be kept private from other users
- Ensure their antivirus software is operational and regularly updated
- Maintain a current backup of any data on their personal device
- Ensure that their device is fully charged each day
- Abide by intellectual property and copyright laws
- Use internet filtering while at school
- Ensure device is not used by another person (for any reason)

Parents and Caregivers

- Provide a mobile computer device for the student that complies with the minimum hardware and software specification indicated by the school
- Consider purchasing a commercial grade antivirus software program, ensuring that it has been installed, is operational and regularly updated on the student's device (Highly recommended by school)
- Provide appropriate software for students to use on their device (eg. MS Office)
- Acknowledge that the core purpose of the student's device at school is to assist the student in their school studies
- Agree that the student uses the department's internet filtering provisions, when using the internet at school (the student does not use their mobile phone as a hot spot)
- Encourage and support appropriate digital citizenship and cyber safety guidelines with students
- Be responsible for repairing any damage that may occur to the student's device
- Provide a protective backpack or case for the student's device
- Are aware of the warranty conditions for the student's device
- Have considered (and preferably purchased) an Accide`ntal Insurance Policy for the student's device
- Listed the student's device under their Home and Contents Insurance Policy (recommended)

Parents and students need to be aware that the school's BYOD program does not support the following:

- Providing technical support for the student's device
- Charging the device at school
- Security, integrity, insurance and maintenance of the student's device
- Cost of repairs if the device is damaged at school
- Backing up data on the student's device
- Provision of software on the student's device

Students and parents/caregivers are asked to lend their support to this very valuable and innovative program. Strong support is paramount to ensure the program is successful and the students gain maximum benefits for their learning.

CONNECTING DEVICE TO SCHOOL COMPUTER NETWORK

Instructions for connecting personal devices to the school computer network can be found on the schools web site: http://pimlicoshs.eq.edu.au

With the website opened, click on the Curriculum option (Menu Bar), then click on Bring Your Own Device option.

The following can also be found in the BYOD section:

- BYOD Instructional Videos
- Windows version installation guide
- MacOS version installation guide
- iOS (iPad) version installation guide