Pacific Paradise State School

Years 4, 5 and 6

Bring Your Own Laptop Charter 2025

Contents

Bring Your Own Laptop Overview

'Bring Your Own (BYO)' Laptop is a new pathway supporting the delivery of 21st century learning. It is a term used to describe a digital device ownership model where students or staff use their personally-owned mobile devices to access the department's information and communication (ICT) network.

Access to the department's ICT network is provided only if the mobile device meets the department's security requirements which, at a minimum, requires that anti-virus software has been installed, is running and is kept updated on the device.

Students and Parents are responsible for the security, integrity, insurance and maintenance of their personal devices and their private network accounts.

The BYO Laptop acronym used by the department refers to the teaching and learning environment in Queensland state schools where personally-owned mobile devices are used. BYO represents more than a personally-owned mobile device; it also includes software, applications, connectivity or carriage service.

The department has carried out extensive BYO Laptop research within Queensland state schools. The research built on and acknowledged the distance travelled in implementing 1-to-1 computer to student ratio classes across the state, and other major technology rollouts.

We have chosen to support the implementation of a BYO Laptop model because:

- BYO Laptop recognises the demand for seamless movement between school, work, home and play
- Our BYO Laptop program assists students to improve their learning outcomes in a contemporary educational setting
- Assisting students to become responsible digital citizens enhances the teaching learning process and achievement of student outcomes as well as the skills and experiences that will prepare them for their future studies and careers.

Pacific Paradise State School highly values the engaging and rich learning experiences that effective technology integration can bring.

The promotion and advancement of Bring Your Own Laptop aligns with worldwide educational trends to ensure today's learners are more adept at communication, creating, collaborating and critically thinking in a technology driven world.

Access to technology through a Bring Your Own Laptop program has changed how we communicate, think and process information.

Digital technologies can maximize learning opportunities and support learning that is connected, collaborative and global. Children at Pacific Paradise will learn how to engage with the world around them and acquire digital skills to participate in life and work beyond school, this includes:

- Access to quality resources
- Learn anytime, anywhere
- Self-directed learning
- Connecting and collaborating
- Developing digital skills
- Accessing & reviewing in real-time
- Connecting families to learning
- Crossing educational divides

Think for a moment of the world in which we live and consider the statistics:

- People are creating 2000 new websites every hour.
- Uploading 35 hours of video every minute.
- Watching 2 billion YouTube videos every day.
- Communicating with people thousands of kilometres away as if they were in the same room.
- They consume, produce and communicate information in previously unimaginable ways.
- As educators we are building 21st century skills, using enabling technologies and personalising learning to engage students in diverse and creative ways.

Parent and Student Responsibilities

Read this Charter so that you are aware of the requirements to participate in the 2025 Bring Your Own laptop program.

Fill in the online digital permission form (QParents)

Provide a laptop that meets our minimum device requirements:

- it is very important to read the minimum device requirements, on page 9 of this Charter so that the laptop you purchase is compatible with our school requirements.

Understand that it is advised that the device has a next day on site repair warranty and/or accidental damage repair

- Understand that Pacific Paradise State School recommends that the laptop purchased to use in the BYO program has accidental damage protection and that the school will take necessary and reasonable precautions to ensure your device is safe, but we cannot be held responsible for any accidental, malicious or deliberate damage or theft.

Have up to date security installed on device, Windows Defender is free with Windows 10 or Windows 11 and works amazingly, Other Antivirus Software like Norton etc can cause disruptions in the usage of the device on the School ICT network.

The laptop is 'G' rated and contains no inappropriate content

- including photos, videos, games, screen savers etc.

The Bring Your Own Laptop must not have a VPN (Virtual Private Network) installed.

- This may stop connection to our school's internet deeming the laptop unsuitable for our program.

Be aware that the ICT facilities should be utilised with good behaviour as stipulated under the Code of School Behaviour; and those students breaking these rules will be subject to appropriate action by the school.

- This may include restricted network access, or loss of BYO privilege, for a period as deemed appropriate by the school.
- Agree to move all games/ programs that are not required, by the class teacher or school, into a separate folder on the laptop and that your child has been instructed not to access those games/programs at school.

Read more here: Code of School Behaviour

Some students may forget their passcode (if you have one) and need assistance from their teacher

- Agree to share the laptop passcode with the class teacher if required.

The laptop is brought to school each day fully charged

- Chargers are not permitted to be used at the school due to WHS Standards.

Connect to the School Organisation and Install Microsoft Office (Free for Students)

- Enrol Device with Windows 10 VIDEO | DOCUMENT
- Enrol Device with Windows 11 VIDEO | DOCUMENT
- Enrol Mac Laptop (MacBook Air or Pro) VIDEO | DOCUMENT

Responsible use of BYO Laptop

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

Responsibilities of participants involved in the Bring Your Own Laptop program

School

BYO Laptop program information, including information on (but not responsible for) connection, care of device at school, workplace health and safety, appropriate digital citizenship and cyber safety:

- network connection at school
- internet filtering (when connected via the school's computer network)
- some technical support (please consult technical support table (on page 16 of this Charter)
- some school-supplied software e.g., Microsoft Office 365
- providing lockable storage for laptops when not in use

Student

- acknowledgement that core purpose of device at school is for educational purposes
- care of device
- appropriate digital citizenship and online safety- for more details, visit the website of the Australian eSafety Commissioner
- security and password protection — password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g., a student should not share their username and password with fellow students)
- some technical support (please consult technical support table below)
- maintaining a current back-up of data
- charging of device

- abiding by intellectual property and copyright laws (including software/media piracy)
- internet filtering (when not connected to the school's network)
- ensuring personal login account will not be shared with another student, and device will not be shared with another student for any reason
- aware that non-compliance or irresponsible behaviour, as per the intent of the BYO Charter and the
- Pacific Paradise State School Student Code of Conduct will result in consequences relative to the behaviour.

Parents and caregivers

- acknowledgement that core purpose of device at school is for educational purposes
- internet filtering (when not connected to the school's network)
- encourage and support appropriate digital citizenship and cyber safety with students (for more details, visit the website of the Australian eSafety Commissioner)

- some technical support (please consult technical support table)
- required software, including sufficient anti-virus/ security software
- protective backpack or case for the device
- adequate warranty and insurance of the device
- aware that non-compliance or irresponsible behaviour, as per the intent of the BYOx Charter and the Responsible Behaviour Plan, will result in consequences relative to the behaviour.

The following are examples of responsible use of devices by students:

- engagement in class work and assignments set by teachers
- developing appropriate 21st Century knowledge, skills and behaviours
- authoring text, artwork, audio and visual material for publication on the Intranet or Internet for educational purposes as supervised and approved 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, encyclopedias, etc.
- researching and learning through the school's eLearning environment
- ensuring the device is fully charged before bringing it to school to enable continuity of learning.
- Be courteous, considerate and respectful of others when using a mobile device.
- Switch off and place out of sight the laptop during classes, where these laptops are not being used in a teacher directed activity to enhance learning.
- Seek teacher's approval where they wish to use a laptop under special circumstances.

The following are examples of irresponsible use of laptops by students:

- using the laptop in an unlawful manner
- use the personal laptop for private use before or after school, or during recess and lunch breaks
- creating, participating in or circulating content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disabling settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
- downloading (or using unauthorised software for), distributing or publishing of offensive messages or pictures
- using obscene, inflammatory, racist, discriminatory or derogatory language
- using language and/or threats of violence that may amount to bullying and/or harassment, or even stalking
- insulting, harassing or attacking others or using obscene or abusive language
- deliberately wasting printing and internet resources
- intentionally damaging any devices, accessories, peripherals, printers or network equipment
- committing plagiarism or violate copyright laws

- using unsupervised internet chat
- sending chain letters or spam email (junk mail)
- accessing private 3G/4G networks during lesson time
- knowingly downloading viruses or any other programs capable of breaching the department's network security
- using the laptop's camera anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets
- invading someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g., forwarding, texting, uploading, Bluetooth use etc.) of such material
- using the laptop (including those with Bluetooth functionality) to cheat during exams or assessments
- take into or use laptop at exams or during class assessment unless expressly permitted by school staff.

Information sent from our school network contributes to the community perception of the school. All students using our ICT facilities are encouraged to conduct themselves as positive ambassadors for our school.

- Students using the system must not at any time attempt to access other computer systems, accounts or unauthorised network drives or files or to access other people's devices without their permission and without them present.
- Students must not record, photograph or film any students or school personnel without the express permission of the individual/s concerned and the supervising teacher.
- Students must get permission before copying files from another user. Copying files or passwords belonging to another user without their express permission may constitute plagiarism and/or theft.
- Students need to understand copying of software, information, graphics, or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.
- Parents and caregivers need to be aware that damage to mobile devices owned by other students or staff may result in significant consequences in relation to breaches of expectations and guidelines in the school's Pacific Paradise State School Student Code of Conduct and the Code of School Behaviour.
- The school will educate students on cyber bullying, safe internet and email practices and health and safety regarding the physical use of electronic devices. Students have a responsibility to incorporate these safe practices in their daily behaviour at school.

The school's Bring Your Own Laptop program supports personally-owned laptops in terms of access to:

- Internet & School Network

However, the school's Bring Your Own Laptop program does not support personally-owned laptops in regard to:

- technical support
- charging of devices at school
- security, integrity, insurance and maintenance
- private network accounts

Device Selection

Students in Year 4, 5 and 6 will require their device on a daily basis.

We understand it is difficult to choose the right device for your student, so below you will find the minimum recommended specifications designed to ensure the device will work at our school.

We are unable to recommend one particular device over another due to our adherence to the "Public Sector Ethics Act 1994" where we have a, "duty to provide advice which is objective, independent, apolitical and impartial".

Here are the Minimum Specifications for Windows 11:

Processor	1 gigahertz (GHz) or faster with 2 or more cores on a compatible 64-bit processor
RAM	4 gigabyte (GB)
Storage	64 GB or larger storage device
System firmware	UEFI and Secure Boot capable
TPM	Trusted Platform Module (TPM) version 2.0
Graphics card	Compatible with DirectX 12 or later with WDDM 2.0 driver
Display	High definition (720p) display that is greater than 9" diagonally and 8 bits per colour channel

Here are the Recommended Specifications for Windows 11:

Processor	i3/i5 Processor
RAM	8 gigabyte (GB)
Storage	256 GB or larger storage device
System firmware	UEFI and Secure Boot capable
TPM	Trusted Platform Module (TPM) version 2.0
Graphics card	Compatible with DirectX 12 or later with WDDM 2.0 driver
Display	High definition (1080p) display that is greater than 13" diagonally and 8 bits per colour channel

In order to provide a consistent experience for students, it is important the laptop meets the minimum standards outlined below, this will ensure the device is able to connect to the school network and ensure that digital content used in the classroom is compatible with the chosen laptop.

Please do not purchase a device unless you are sure the device meets the following specifications.

- Windows 11 (not in S Mode)

or

- Mac (minimum operation system: macOS 12 Monterey)
- 6 hour battery (no charging at school- don't bring charger)
- Dual Band WiFi: 5 GHz compatible essential

Our School has 5 GHz WiFi only. 2.4 GHz is not available

We do not support: *Apple iPads, Google Chromebook, Microsoft Surface RT, Android tablets. These devices are not compatible with our Bring Your Own Laptop program offered to Years 4, 5 and 6 in 2025.

We have had several incidences in 2018- 2024 with family monitoring programs. These security programs have steps that families can take to monitor and restrict students particularly connecting to the internet. At school students are required to connect to the internet and some activities and work is set up by the classroom teachers online. These family monitoring/ security programs have blocked the students from connecting to the school internet and some families have needed to turn off the service to enable students to use their laptop to access their work at school. We require students to access our highly filtered safe internet at school.

If the laptop is going to be used in future years at High School, please check on each school's website for their device requirements as they do change from school to school.

The cost of laptops can vary greatly so when purchasing a laptop please keep in mind that you do get what you pay for. If purchasing a cheap laptop that meets our device requirements be aware that it may operate slowly compared to a laptop with higher specifications.

It is required that all BYO Laptops have some form of protective casing. This will minimise the likelihood of damage as students travel to and from school. (This is not provided by the school).

We will provide a lockable cupboard for students in each class to securely store devices when not in use.

Device care, Theft, Loss and Accidental Damage Insurance

The student is responsible for taking care of and securing the device and accessories in accordance with school policy and guidelines. Responsibility for loss or damage of a device at home, in transit or at school belongs to the student. It is important that student devices are

insured against theft and accidental damage. This is often possible as an extension of your home and contents insurance, as a separate policy or as a part of a package at the time of purchase from the vendor. The school will take necessary and reasonable precautions to ensure your device is safe, but we cannot be held responsible for accidental damage or theft. It is advised that accidental damage and warranty policies are discussed at point of purchase to minimise financial impact and disruption to learning should a device not be operational.

Pacific Paradise State School recommends that the laptop purchased to use in the BYO program has accidental damage protection and that the school will take necessary and reasonable precautions to ensure your device is safe, but we cannot be held responsible for any accidental, malicious or deliberate damage or theft.

School technology support staff or teachers will not support, repair or troubleshoot student devices other than to connect the device to the school Wi-Fi.

General precautions

- Food or drink should never be placed near the device.
- Using the laptop before school, at break times or after school, on school grounds is not allowed unless supervised by the student's teacher.
- Plugs, cords and cables should be inserted and removed carefully.
- Devices should be carried within their protective case where appropriate.
- Carrying devices with the screen open should be avoided.
- Ensure the battery is fully charged each day.
- Turn the device off before placing it in its bag.

Protecting the screen

- Avoid poking at the screen — even a touch screen only requires a light touch.
- Don't place pressure on the lid of the device when it is closed.
- Avoid placing anything on the keyboard before closing the lid.
- Avoid placing anything in the carry case that could press against the cover.
- Only clean the screen with a clean, soft, dry cloth or an anti-static cloth.
- Don't clean the screen with a household cleaning product.

Data security and back-ups

As we all know, technology can fail and can be lost or stolen so it is extremely important that students have a backup plan in case things go wrong.

Backing up is easy. Once set up, your data should be backing up automatically. You just need to check every once in a while, to make sure your backups actually work. There are three main types of backup solutions:

- Local Backup
    - It is your responsibility to back up any important files. Options for back up include to copy your most important files onto an external hard drive or save and sync to OneDrive for Students.
- Offsite Backup

    - This is another automatic backup or an external hard drive that's stored at another location, such as a friend's house. This protects your backup in case of theft, natural disaster or simple hardware failure.
- OneDrive
    - Students at our school have access to Microsoft's OneDrive for Business through the MIS Gateway.
    - OneDrive for Business provides a secure place on the internet where school-related files can be stored, shared and synced.
    - Students across all year levels will gain access providing they have at least a 0.1 FTE enrolment at our school. Each student will gain access to:
        - OneDrive for Business library with one terabyte of storage per person.
        - Expanded suite of Office Online web applications, including OneNote, Word, PowerPoint and Excel.
        - Education Queensland eBooks Digital Library

Passwords

Use of the school's ICT network is secured with a user name and password. The password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g. a student should not share their username and password with fellow students).

The password should be changed regularly, as well as when prompted by the department or when known by another user.

Personal accounts are not to be shared. Students should not allow others to use their personal account for any reason.

Students should log off at the end of each session to ensure no one else can use their account or device.

Students should also set a password for access to their BYO Laptop and keep it private.

Parents/caregivers may also choose to maintain a password on a personally-owned device for access to the device in the event their student forgets their password or if access is required for technical support. Some devices may support the use of parental controls with such use being the responsibility of the parent/caregiver.

Digital Citizenship

Students should be conscious creators of the content and behaviours they exhibit online and take active responsibility for building a positive online reputation. They should be conscious of the way they portray themselves, and the way they treat others online.

Students should be mindful that the content and behaviours they have online are easily searchable and accessible. This content may form a permanent online record into the future.

Interactions within digital communities and environments should mirror normal interpersonal expectations and behavioural guidelines, such as when in a class or the broader community.

Parents are requested to ensure that their child understands this responsibility and expectation. The school's Student Code of Conduct also supports students by providing school related expectations, guidelines and consequences.

Cyber Safety

If a student believes they have received a computer virus, spam (unsolicited email), or they have received a message or other online content that is inappropriate or makes them feel uncomfortable, they must inform their teacher, parent or caregiver or report the incident as soon as is possible.

Students must also seek advice if another user seeks personal information, asks to be telephoned, 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, caregivers and students are encouraged to read the department's Cybersafety and Cyberbullying guide for parents and caregivers. This guide published by the department provides important information for parents about cyber safety and cyberbullying. It suggests what parents and caregivers could do if their child is the target or is responsible for inappropriate online behaviour.

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 students, while using ICT facilities and devices, will be required to act in line with the requirements of the Code of School Behaviour and any specific rules of the school. To help protect students (and staff) from malicious web activity and inappropriate websites, the school operates a comprehensive web

filtering system. Any device connected to the internet through the school 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 websites including those that do not disclose information about their purpose and content. The school's filtering approach represents global best-practice in internet protection measures. However, despite internal departmental controls to manage content on 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 DET network must also be reported to the school.

The 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 appropriate internet use by students outside the school.

Parents, caregivers and students are also encouraged to visit the Australian Government eSafety website for resources and practical advice to help young people safely enjoy the online world.

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 etc. 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 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 without warning and be subject to prosecution from agencies to enforce such copyrights.

Software

Schools may recommend software applications in order to meet the curriculum needs of particular subjects. Parents/caregivers may be required to install and support the appropriate use of the software in accordance with guidelines provided by the school. This includes the understanding that software may need to be removed from the device upon the cancellation of student enrolment, transfer or graduation.

Security program for laptop

Access to the department's ICT network is provided only if the laptop meets the department's security requirements which, at a minimum, requires that anti-virus software has been installed, is running and is kept updated on the device.

Windows Defender (free with Windows 11)

https://www.microsoft.com/en-au/windows/comprehensive-security

Please note some security software is not compatible with the DET network.

We have had several incidences in 2018- 2024 with Family Monitoring programs. These security programs have steps that families can take to highly monitor and restrict students particularly connecting to the internet. At school students are required to connect to the internet and some activities and work is set up by the classroom teachers online. These programs have blocked the students from connecting to the school internet and some families have needed to turn off the service to enable students to use their laptop to access their work. We require students to access our highly filtered safe internet at school.

Monitoring and Reporting

Students should be aware that all use of internet and online communication services can be audited and traced to the account of the user.

All material on the 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 holdings associated with its use.

Misuse and Breaches of Acceptable Usage

Students should be aware that they are held responsible for their actions while using 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/remove access of personally owned laptops to the intranet, internet, email or other network facilities 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 laptops may result in disciplinary action which includes, but is not limited to, the withdrawal of access to school supplied services.

School Technical Support

School technicians are only able to provide a specific level of support for BYO devices because of the range of devices able to be used within the school.

Technical support is limited to:

- Connection of the device to the school wireless network if there is a problem after classroom teacher gives students permission and instructions
- School technicians are not able to support students with (but not limited to):
    - Hardware faults,
    - Windows / Mac OS software issue
    - Physical damage to your device,
    - Issues caused by viruses. (Where a device potentially threatens the school network, it may be temporarily or permanently suspended from connecting).

Technical Support

	Connection:	Hardware:	Software:
Parents and Caregivers	✓ (home-provided internet connection)	✓	✓
Students	✓	✓	✓
School	✓ school provided internet connection	(dependent on school-based hardware arrangements)	✓ (some school-based software arrangements)
Device vendor		✓ (see specifics of warranty on purchase)	

Charging of Devices

Students do not have the opportunity to charge their device during class and it is expected that devices used within the school have sufficient battery power to last an entire day. Your device is to be fully charged before the commencement of each school day. Due to Work Place Health and Safety requirements student's laptop chargers are not allowed at school.

Mobile Network Tethering / 3g 4g Connections

Mobile network tethering, wireless Internet access points and inbuilt data connectivity can provide students with an UNFILTERED network connection within the school grounds. These types of Internet connections need to be disabled before arrival at school as the school cannot monitor or take responsibly for content accessed via these methods.