PACIFIC PARADISE STATE SCHOOL

Laptop Program Charter

☎ 07 5457 2333

✉ admin@pacificparadisess.eq.edu.au

🌐 www.pacificparadisess.eq.edu.au

Follow us on Facebook

CONTENTS

Further Information: admin@pacificparadisess.eq.edu.au

OVERVIEW

Our laptop program at Pacific Paradise State School provides choice and flexibility for our students. It enables students with the potential for anywhere, anytime learning with the use of portable devices. Our Laptop Program consists of the following options.

BYOD (Bring Your Own Device)

Bring your own device (BYOD) is a term used to describe a digital device ownership model where students use their personally owned portable devices to access the Department's information and communication (ICT) network for learning.

Access to the Department's ICT network is provided only if the mobile device meets the Department's security requirements and minimum specifications (refer to 'Minimum Specifications' section below).

Annual School Laptop Hire

The school has a limited number of school owned laptops that we are able to hire on an annual basis to students. These devices are hired on a first in, first served basis.

The **Annual School Laptop Hire** option has a fee of **$275 per annum** (required before laptop can be issued). Pro- rata refunds are based on a full school term, not part thereof ($68.75 term). New enrolments throughout the year are charged in the same manner.

Accidental damage to an Annual Hire Laptop will incur a $55 repair fee. Any loss of an Annual Hire Laptop which is unrecoverable will incur a $200 fee towards its replacement. This also applies for malicious/deliberate damage.

If you would like to be part of this program, please request an application form from the school office.

Student Technology Equity Partnership (STEP) Devices

The school has a limited number of school owned STEP laptops that are able to be assigned to selected students on an annual basis. The STEP initiative is part of the Queensland Government's commitment to narrowing the digital divide and supporting our school's most financially disadvantaged students. In support of the initiative's aims, these devices are provided to selected students in this situation to assist learning, both at school and at home. This will also help teachers teach using this technology and not have inequity being a barrier for classroom teaching and learning.

To be eligible for a STEP device it must be proven that you are not financially capable of purchasing a device for your child to use at school. This is checked by a school representative that has access and the ability to determine this need, their determination will be final.

If you would like to be part of this program and think yourself eligible, please request an application form from the school office to initiate the process.

Accidental damage to a STEP Laptop will incur a $55 repair fee. Any loss of a STEP Laptop which is unrecoverable will incur a $200 fee towards its replacement. This also applies for malicious/deliberate damage.

School Day Hire Loan Devices

Pacific Paradise SS have a limited quantity of Day Hire Laptops that are only available to students participating in either BYOD, Annual Hire or STEP programs should their regular device suffer damage or requires a warranty repair. Written communication is required from parents in these scenarios.

Day Hire laptops are not available for students if they simply forget to bring their device to school or fail to adequately charge their device.

Students are only allowed access to Day Hire Laptops at the beginning of the school day or during break times and must have approval from their classroom teacher. Day Hire Laptops will not be issued during class time and must be returned to the Resource Centre at the end of the school day. Day Hire Laptops are issued at random. We cannot guarantee the same laptop will be available on consecutive days.

Accidental damage to a Day Hire Laptop will incur a $55 repair fee and the loss of a Day Hire Laptop which is unrecoverable will incur a $200 fee towards its replacement. This also applies for malicious/deliberate damage.

BRING YOUR OWN DEVICE (BYOD)

Device Selection

Prior to acquiring a device for use at school the parent/carer and student should be aware of the school's minimum specifications of appropriate device type, operating system requirements and software. These specifications relate to the suitability of the device to enable class activities, meet student needs, meet network requirements and promote safe and secure network access.

Devices may be purchased from any retailer, and most local stores will be familiar with the school's minimum device requirements.

Minimum Specifications

Please ensure you refer to the below MINIMUM requirements when selecting a device for use in the BYOD Program. This is to ensure compatibility with the Department of Education's BYOx Link network and avoid wasted expenditure and disappointment.

Operating System Options:

- Windows 11 or later (Devices in S Mode will be required to switch out of S Mode during Intune enrolment) **Windows 10 is not supported.**
- MacOS 14 or later (Please note, with older MacBooks, the device must be able to support at least the 3 latest MacOS systems. This is due to Microsoft InTune requirements.

⚠ **CAUTION - The the folowing devices are not supported and will not work at school.**
Chromebook, Android devices, Linux devices, iPad mini.

Processor: Intel Celeron or Pentium Core 3 / AMD Ryzen 3

(Not Supported – Qualcomm Snapdragon ARM or equivalent)

Memory: Minimum 8GB RAM

Screen Size: Minimum 11 inch (maximum recommended size: 14")

Hard Drive: Minimum 256GB SSD

Battery Life: Minimum of 6+ hours. Please note it is expected that all devices will be fully charged at the beginning of the school day. **No personal chargers are to be brought to school**.

Keyboard:

- Must have a tactile (physical) keyboard
- Touch screen keyboard alone is **Not Sufficient**

Wireless Adaptor: Must support 802.11ac/802.11ax 5Ghz wireless networks

USB Ports: minimum of 2

Other Considerations:

- Extended warranty / Accidental Damage Protection
- Hard and/or well-padded protective case

- Weight and size factor for student carrying it all day and fitting into school bag
- The student's user account must be an administrator.

NOTE: Microsoft Office is included in your student's DOE user account free of charge

Support Provided by School

- Pacific Paradise State School BYOD program will support filtered Internet access (while connected to the school wireless network), and file access and storage while at school. The school is only able to offer limited technical support/diagnosis of hardware or software issues on privately owned devices.

Responsibility for Care of Device

- 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 recommended that laptops are transported in a strong and if possible waterproof carry case/sleeve.
- It is highly recommended that advice be sought regarding the inclusion of your privately owned device in your home and contents insurance policy for loss and for accidental damage.

Software

When a student signs up for BYOD connectivity, the school will provide information and support with respect to the following software packages where agreements have been entered into between Education Queensland and the vendors for the purpose of providing student software for personally owned devices:

- *Microsoft Office* – every student in Education Queensland schools is entitled to download and install Microsoft Office for **free**.
- *Adobe Express* – All students are issued with a licence to Adobe express. Adobe express applications can be accessed via the Adobe Express website https://new.express.adobe.com/ using their Student DOE email address and password.

Suggestions of additional software you may wish to install

- Antivirus software: Although Windows 10+ devices have *Microsoft Defender* as default virus protection, you may wish to install an alternative antivirus program such as Avast or AVG. Please ensure only 1 antivirus suite is installed – having more than one will cause conflicts. **N.B.** If you install a third-party antivirus, *Microsoft Defender* will automatically "step down".
- We also recommend installing the following free software: Adobe Reader & VLC Player.

GENERAL INFORMATION

Responsibilities of Stakeholders Involved in the Program

The School

- Laptop program induction — including information on connection, care of device at school, appropriate digital citizenship and cybersafety
- Network connection at school
- School network and cloud storage (OneDrive)
- School email address
- Internet filtering (when connected via the school's computer network)
- Technical support for all students (BYOD limitation as laptop is not school owned)
- Free software - Microsoft Office
- Approved online memberships - e.g. Soundswave

Students

- Participation in laptop program induction
- Acknowledgement that core purpose of device at school is for educational purposes
- Care of device
- Appropriate digital citizenship and online cyber safety
- 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
- Maintaining a current back-up of data – especially assessment
- Charging of device – it is expected that students will bring their laptop to school every day, fully charged, in preparation for the day's classes – Personal chargers are not permitted at school
- Abiding by intellectual property and copyright laws (including software/media piracy)
- Internet filtering (when not connected to the school's network)
- Ensuring device will not be shared with another student for any reason
- No use of mobile phones to hot-spot to deliberately circumvent the cyber protections put in place for students on campus by Education Queensland
- Ensure device is only used in the classroom when at school

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)
- Encouraging and supporting appropriate digital citizenship and cyber safety with child
- Ensuring that the child develops the habit of charging the laptop overnight in readiness for the next day's lessons and remembers to bring the device to school
- Providing installation of anti-virus software on BYOD devices
- Protective case for the device
- Adequate warranty/insurance of BYOD devices
- Completion of the Online Services Consent on QParents

Web Filtering

At all times, students while using ICT facilities and devices, will be required to act in line with the requirements of the school's Student Code of Conduct.

To protect students (and staff) from malicious web activity and inappropriate websites, Education Queensland operates a comprehensive web filtering system within their schools. Any device connected to the Internet through the school network will have filtering applied.

The filtering system provides a layer of protection to students and staff against:

- inappropriate web pages
- spyware and malware
- peer-to-peer sessions
- scams and identity theft

Whilst this filtering approach represents global best-practice in Internet protection measures, despite internal departmental controls to manage content on the Internet, illegal, dangerous or offensive information may be accessed or accidentally displayed. 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 QED network must also be reported to the school.

Privately owned devices have access to home and other out of school Internet services which may not include any Internet filtering. Parents/caregivers are encouraged to install a local filtering application (compatible with the school's BYOx network) 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 of school.

In relation to this, students and parents need to be aware of the following:

- Students are not permitted to hot-spot their phones for Internet connectivity, as this negates the very benefits that are designed to protect them from being vulnerable whilst online at school.
- It is totally unacceptable for students to download programs onto their computer that are designed to circumvent the filtering protection provided by Education Queensland on the school campus.
- Using VPN (Virtual Private Network) software **will** conflict with the school wireless connectivity process – i.e. they will not be able to access the Internet or necessary network drives whilst on campus.

Data Security and Back-ups

- Students must understand the importance of backing up data securely. Should a hardware or software fault develop, important assignment work may be lost.
- The student is responsible for the backup of all data. Education Queensland provides every student with approximately 2TB of secure cloud storage (*OneDrive*) which is accessible on and off campus.
- Whilst other forms of back-up such as USB drives, external hard drives are an option, these do not have the security and reliability of *OneDrive*. They are volatile in the sense that they can be damaged, data corrupted and are easily misplaced.
- Students who are part of the school laptop hire program or STEP program should also be aware that in the event that any repairs need to be carried out on the laptop relating to the hard drive, data stored on the local laptop drives could be lost.

Acceptable Computer and Internet Use

Upon enrolment in a Queensland Government school, parental or caregiver permission is sought to give the student(s) access to the internet, based upon the relevant policies of Education Queensland.

Communication through internet and online communication services must comply with the Student Code of Conduct available on the school website.

There are conditions that students are required to adhere to. Students should not:

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

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

Passwords

- Passwords must not be obvious or easily guessed; they must be kept confidential and changed when prompted or when known by another user.
- Personal accounts cannot 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 laptop.

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, accessible and 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 behaviour policies also support students by providing school related expectations, guidelines and consequences.

Cybersafety

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 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 are encouraged to explore and use the *'Cyberbullying help button'* on school devices to talk, report and learn about a range of cyber safety issues. Cyber safety is also addressed in Futures lessons throughout the year.

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 recipient's computer
- chain letters, hoax emails or phishing 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.

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 mobile devices 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 mobile devices may result in disciplinary action which includes, but is not limited to, the withdrawal of access to school supplied services.

Responsible Use

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

- Portable devices on campus should be primarily used for engagement in class work and assignments set by teachers, conducting general research for school activities and projects and communicating or collaborating with other students, teachers, parents, caregivers or experts for educational purposes.
- 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.
- Parents and caregivers need to be aware that damage to portable devices owned by other students or staff may result in significant consequences in relation to breaches of expectations and guidelines in the school's behaviour policies.
- The school will educate students on cyber bullying, safe Internet and email practices. Students have a responsibility to incorporate these safe practices in their daily behaviour at school.
- 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.

When using portable devices, students **MUST NOT**:

- use the device in an unlawful manner
- create or participate in circulating content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disable settings for virus protection, spam and/or Internet filtering that have been applied as part of the school standard
- download (or using unauthorised software for), distributing or publishing of offensive messages or pictures
- use obscene, inflammatory, racist, discriminatory/derogatory or bullying language
- download viruses/other programs capable of breaching the Department's network security

- use the mobile device’s camera or recording functions inappropriately, violating the privacy of other individuals
- covertly use Bluetooth functionality during lessons or exams
- hotspot their phone to bypass the school’s protective filtering designed to ensure cyber safety
- 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.

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. Students must not trespass in another person's files, home drive, email or access 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 and be subject to prosecution from agencies to enforce such copyrights.

BYOD AGREEMENT

This BYOD Agreement form must be signed and returned to the school before a device can be connected to the school network. The student and parent or caregiver must carefully read this agreement and the School Laptop Program Charter before signing it. Any questions should be addressed to the school and clarification obtained before the agreement is signed.

In signing below, I acknowledge that I,

☐ accept all policies and guidelines as per the School's Student Code of Conduct

☐ accept all policies and guidelines as per the ICT Acceptable Use Policy

☐ acknowledge that I understand and agree with all of the conditions detailed in the School Laptop Program Charter

☐ and of particular note, I:

- understand the device is not protected by the school's Internet filtering system when connected to a wireless network outside of school,
- will ensure the device arrives at school fully charged each day,
- will ensure that all web browsers and tabs are closed prior to arriving at school,
- understand that failure to comply with the conditions of the Laptop Program Charter will prevent the device from being used at school,
- understand it is my responsibility to insure the device against theft, damage or loss and I understand the potential costs involved as a result of damage to the device,
- understand that I may not connect to a mobile data network connection (e.g. 4G/5G) when at school and will ensure that this feature is disabled prior to coming to school.

STUDENT NAME ______________________________

PARENT/GUARDIANS NAME ______________________ **DATE** __________

SIGNATURE ______________________________