Engaging Minds, Empowering Futures

BYO Laptop Charter

Years 4, 5 and 6 2019

Pacific Paradise State School

Contents

Personally-owned mobile device charter

BYO 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 Advice for State Schools on Acceptable use of ICT Facilities and Devices.

Students and staff are responsible for the security, integrity, insurance and maintenance of their personal mobile 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.

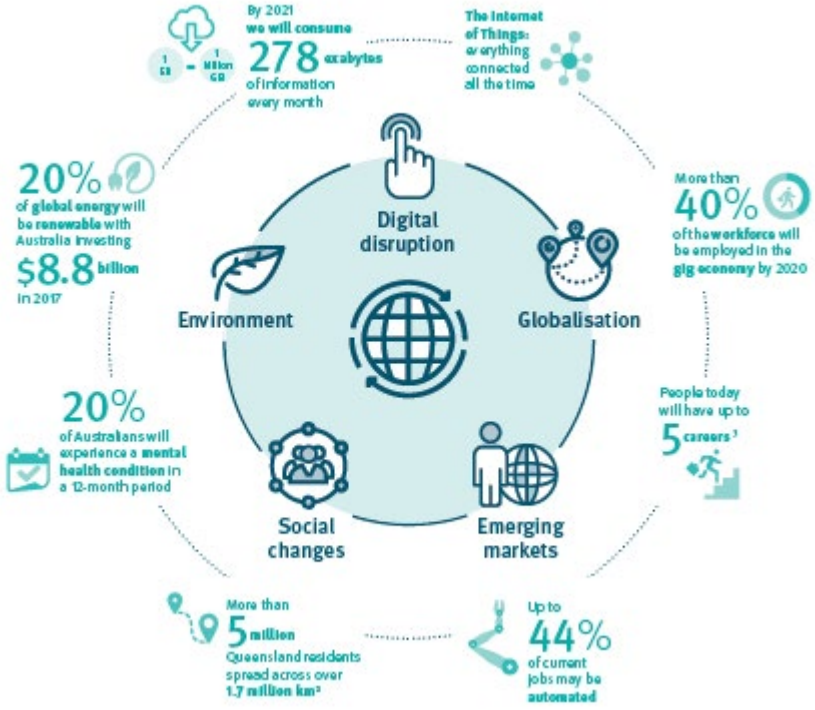
* Watching 2 billion YouTube videos every day.

* They connect 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.

The Department of Education has recently released the latest update to the Strategic Plan, something it does every year to ensure a consistency of vision within an ever changing world. This year, the Department of Education, has included some statistics that influence how we teach and learn.



Parents/ students responsibilities

- Provide a device e.g. laptop that meets requirements e.g. dual band Wi-Fi (see minimum device requirements for more).
- Understand that it is advised that the device has a next day on site repair warranty e.g. Acer/ Dell offer this at time of purchase.
- Have up to date security installed on device e.g. Norton ($9.50 per year) (install/ access via The Learning Place, Windows Defender (free) with Windows 10
- Have Microsoft Office installed (free for all state school students)
- Read and sign the Responsible Use Agreement on the last page of this charter.

Norton Antivirus

To purchase your Norton Antivirus software, or browse the product pricing and information, visit The Learning Place click the rolling banner ad Norton by Symantec link on the top left side the page and follow the instructions.

Note: The Norton by Symantec URL will only work when accessed from departmental pages, such as The Learning Place, when you are outside of the DET network.

- Device is brought to school each day fully charged
- Install Microsoft office Free for students (www.education.qld.gov.au/office2016)

Sign the behaviour acceptable use agreement (on the last page of this charter) and return to your teacher immediately. Devices cannot be brought to school and connected until a signed agreement is returned.

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 well within the School.

Unfortunately, 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".

Minimum Device Specifications

In order to provide a consistent experience for students, it is important the device 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 device. Please do not purchase a device unless you are sure the device meets the following specifications.

***Windows 10 or if a Mac minimum MacOS Sierra 10.12**

***6 hour battery (no charging at school- don't bring charger)**

***Dual Band WiFi: 2.4 & 5 GHz**

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.

	High end laptop	Low end laptop
RAM	4+Gb	< 2Gb
Storage	320+Gb	< 250 Gb
CPU	> Intel Core i5	< Intel Core i5
Wireless	WiFi (b/g/n) 2.4GHz & 5.0GHz	WiFi (b/g/n) 2.4GHz & 5.0GHz

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.
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 2019

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.

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

General precautions

- Food or drink should never be placed near the device.
- 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

Every week, copy your most important files onto an external hard drive next to your desk, in your cupboard, or any other place where you can easily retrieve it.
You can even use Windows Backup (or Time Machine, if you have a Mac) to do this automatically.

Offsite Backup

This is another automatic backup or an external hard drive that's stored at another location, such as a friend or family's house. This protects your backup in case of theft, natural disaster or simple hardware failure.

Cloud Backup

Similar to an offsite backup, this involves simply installing a small app (eg. Dropbox, Google Drive, Microsoft OneDrive) on your computer to instantly and automatically copy your files to the internet. This makes multiple copies of your files at various places around the world, making it hard to lose any of your files.

It's super simple and done instantly - you barely need to do anything. However, your backups can be a little bit of a pain to retrieve though (it's a lot of stuff you have to download) so having this option in conjunction with one of the above is a good, secure plan.

OneDrive

Students at our school have access 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 your school. Each student will gain access to:

- OneDrive for Business library with five terabytes of storage per person.
- An expanded suite of Office Online web applications, including OneNote, Word, PowerPoint and Excel.

Acceptable personal mobile device 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 policy contained within the Acceptable Use of the Department's Information, Communication and Technology (ICT) Network and Systems

This policy also forms part of this Student Laptop Charter. The acceptable-use conditions apply to the use of the device and internet both on and off the school grounds.

Communication through internet and online communication services must also comply with the department's Code of School Behaviour and the Responsible Behaviour Plan available on the school website.

While on the school network, 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 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.

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

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 Responsible Behaviour Plan also supports 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 'Cybersafety Help button' to talk, report and learn about a range of cybersafety issues.

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.

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 Communications and Media Authority's CyberSmart 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.

Microsoft Office 365

All Queensland State School students have access to register for a free copy of Microsoft Office365. Once registered, students will be able to download the Office365 suite and can install on 5 separate devices.

In order for students to take advantage of this offer they will require an active MIS login and school email account.

How long can a student leverage Office 365?

Students can leverage this until they graduate or are no longer attending Pacific Paradise State School. At that point, you must disable your Office 365 license on any device it was installed.

Suggestion of additional software to install:

Internet Browsers
• Google Chrome http://www.google.com/chrome

• Mozilla Firefox http://www.getfirefox.com

• Internet Explorer https://www.microsoft.com/en-au/download/internet-explorer.aspx

Plugins
• Adobe Flash, Reader, Air, Shockwave Player www.adobe.com

• Java - http://www.java.com/en/download/index.jsp

Online Storage/Backup
•OneDrive for Business through the MIS gateway

Video Players:
• Quicktime Player http://www.apple.com/quicktime/download/

• VLC Player http://www.videolan.org/vlc/

Audio Recorder:
• Audacity http://audacity.sourceforge.net/download/

Virus / Malware Protection:

• Microsoft Security Essentials http://windows.microsoft.com/en-us/windows/security-essentials-download

• Malwarebytes http://www.malwarebytes.org

• Please note some security software is not compatible with the DETE network (eg. Bullguard).

• Norton Security – see page 4 of this document for instructions

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 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.

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
- 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. WH&S requirement limit the availability of access to charging stations within the School. The school is unable to provide power adaptors for individual devices.

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

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 stakeholders involved in the BYO Laptop program:

School

- BYO Laptop program induction — including information on (but not responsible for) connection, care of device at school, workplace health and safety, appropriate digital citizenship and cybersafety
- network connection at school
- internet filtering (when connected via the school's computer network)
- some technical support (please consult Technical support table below)
- some school-supplied software e.g. Adobe, Microsoft Office 365 …
- providing lockable storage for laptops when not in use

Student

- participation in BYO Laptop program induction
- acknowledgement that core purpose of device at school is for educational purposes
- care of device
- appropriate digital citizenship and online safety (for more details, see ACMA CyberSmart)

- 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
- understanding and signing the BYO Laptop Charter Agreement.

Parents and caregivers

- participation in BYO Laptop program induction
- 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 cybersafety with students (for more details, see ACMA CyberSmart)
- some technical support (please consult Technical support table)
- required software, including sufficient anti-virus software
- protective backpack or case for the device
- adequate warranty and insurance of the device
- understanding and signing the BYO 2019 Laptop Charter Agreement.

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

- Use mobile devices for:
  - 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 mobile device during classes, where these devices are not being used in a teacher directed activity to enhance learning.
- Use the personal mobile device for private use before or after school, or during recess and lunch breaks.

- Seek teacher's approval where they wish to use a mobile device under special circumstances.

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

- using the device in an unlawful manner
- 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 mobile device'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 mobile device (including those with Bluetooth functionality) to cheat during exams or assessments
- take into or use mobile devices at exams or during class assessment unless expressly permitted by school staff.

In addition to this:

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 Responsible Behaviour Plan.
- 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 BYO Laptop program supports personally-owned mobile devices in terms of access to:

- internet

However, the school's BYO Laptop program does not support personally-owned mobile devices in regard to:

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

Responsible use agreement 2019

The following is to be read and completed by both the STUDENT and PARENT/CAREGIVER:

- I have read and understood the BYO 2019 Laptop Charter and the school Responsible Behaviour Plan.
- I agree to abide by the guidelines outlined by both documents.
- I am aware that non-compliance or irresponsible behavior, as per the intent of the BYO Laptop Charter and the Responsible Behaviour Plan, will result in consequences relative to the behaviour.

Please fill in the following details:

Laptop Brand and Model: _____

Protective Case: Yes ☐ (tick)

Operation System eg Windows 10 or Sierra:_____

Security program eg Norton: _____

Microsoft Office installed: Yes ☐ if not please provide reason

_____

Accidental Damage Protection: Yes ☐

Does this laptop meet the minimum Device specifications stated on page 7 of this document: Yes ☐

if not please provide reason _____

Student's name: _____ Date:

Student's Year Level in 2019:_____

Student's signature:_____ Date:

Parent's/caregiver's name: _____ Date:

Parent's/caregiver's signature: _____Date:

*this form must be filled in and handed to the class teacher before the laptop can be brought to school