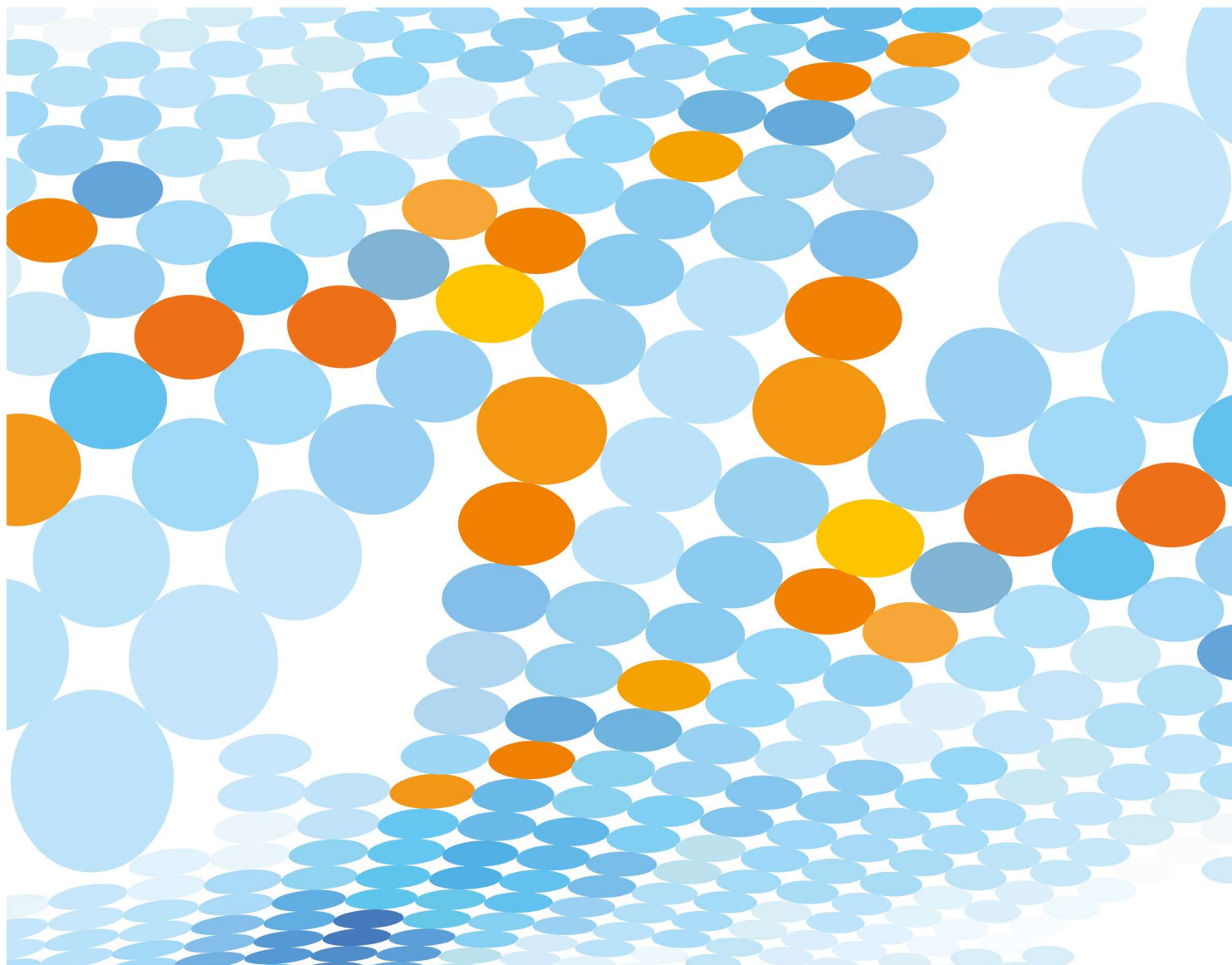


# Pioneer State High School

## Student BYOx Charter



# Contents

BYOx overview .....	3
Device selection .....	3
Device care.....	4
Data security and back-ups.....	4
Acceptable personal device use.....	5
Passwords .....	5
Digital citizenship .....	5
Cybersafety .....	6
Web filtering .....	6
Privacy and confidentiality.....	7
Intellectual property and copyright .....	7
Software .....	7
Monitoring and reporting .....	7
Misuse and breaches of acceptable usage .....	7
Responsible use of BYOx.....	7
Loan Equipment .....	10
Responsible use agreement.....	10

## BYOx overview

Pioneer State High is implementing a Bring Your Own 'x' (BYOx) program to support the delivery of 21st century learning to students.

BYOx is a term used to describe a digital device ownership model where students use their personally-owned devices to access the department's information and communication (ICT) network.

These devices include laptops and tablets however not mobile phones. Access to the department's ICT network is provided only if the 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 are responsible for the security, integrity, insurance and maintenance of their personal devices and their private network accounts.

Pioneer SHS has chosen to implement the BYOx model because:

- We recognise the demand for seamless movement between school, work, home and play.
- Our BYOx program assists students to improve their learning outcomes in a contemporary educational setting.
- Our BYOx program assists students to become responsible digital citizens and 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.

## Device selection

Before acquiring a device to use at school the parent or caregiver and student should be aware of the school's specification of appropriate device type, including operating system requirements and software requirements.

The school's BYOx program will support printing, filtered internet access, and file access through the department's network while at school. The school's BYOx program does not include school technical support or charging of devices at school.

While Apple MacOS devices and iPads are acceptable, compatibility issues with our network can cause issues connecting to some school resources.

The minimum specifications of the device can be found below;

Laptops minimum specifications :	
Screen size:	Between 12" to 16"
Processor	Intel Core I3 or above ( or Equivalent for Apple MacOS 15 )
RAM:	8GB
Storage:	256GB or above
Wireless:	5GHz compatible (802.11n/ac/ax) - <b>mandatory</b>
Operating System:	Windows: Windows 11 (running all latest updates) Apple MacBook: MacOS 15 (Sequoia) and above  <b>Please note - Windows 10 is now obsolete and incompatible with the school's systems</b>
Battery	Capable of 6+ hours of usage
Accessories	<ul style="list-style-type: none"> <li>• External USB/Bluetooth mouse (If your student prefers, to use over touchpad)</li> <li>• Hard laptop case (to protect laptop).</li> </ul>
Warranty / Insurance	Accidental Damage Protection (ADP) insurance (or AppleCare+ for Apple devices) is highly recommended to cover for damage caused to said BYO device.

<b>iPads minimum specifications :</b>	
Screen size:	Standard iPad or above (not iPad Mini)
Storage:	64GB or above
Wireless:	Wi-Fi only iPads
Operating System:	iPadOS 17 or later
Battery:	Capable of 6+ hours of usage
Peripherals:	<ul style="list-style-type: none"> <li>Physical keyboard</li> <li>Hard iPad case and screen protector (to protect iPad)</li> </ul>
Warranty / Insurance	AppleCare+ insurance is highly recommended to cover for damage caused to said BYO device.

### Device care

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. Advice should be sought regarding inclusion in home and contents insurance policy.

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.

### 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 BEFORE arriving at school.
- 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

Students must ensure they have a process of backing up data securely. Otherwise, should a hardware or software fault occur, assignments and the products of other class activities may be lost.

The student is responsible for the backup of all data. While at school, students may be able to save data to the school's network, which is safeguarded by a scheduled backup solution. All files must be scanned using appropriate anti-virus software before being downloaded to the department's ICT network.

Students are also able to save data locally to their device for use away from the school network. The backup of this data is the responsibility of the student and should be backed-up on an external device, such as an external hard drive or USB drive.

Students should also be aware that, in the event that any repairs need to be carried out the service agents may not guarantee the security or retention of the data. For example, the contents of the device may be deleted and the storage media reformatted.

**Please Note. Pioneer State High School is not responsible for students who DO NOT have adequate backups and students WILL NOT be granted assessment extensions due to their work being lost by not having an adequate backup of their work.**

### Acceptable personal 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 Student Code of Conduct 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, music or videos
- 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 BYOx device 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 website of the Australian eSafety Commissioner](#) 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.

## 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.

## Responsible use of BYOx

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 BYOx program

### School

BYOx 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)
- limited technical support (please consult Technical support table below)
- limited school-supplied software e.g. Adobe, Microsoft Office 365 ...
- printing facilities
- school representative signing of BYOx Charter Agreement.

### Student

- participation in BYOx 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, [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
- understanding and signing the BYOx Charter Agreement.

### Parents and caregivers

- participation in BYOx 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, [visit the website of the Australian eSafety Commissioner](#))
- some technical support (please consult Technical support table below)
- 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 BYOx Charter Agreement.

### 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)	



**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, encyclopaedias, 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 mobile phone devices

**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
- bypassing the schools filtering service
- 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/5G networks.
- knowingly downloading viruses or any other programs capable of breaching the department's network security
- using the 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 device (including those with Bluetooth functionality) to cheat during exams or assessments.
- take into or use devices at exams or during class assessment unless expressly permitted by school staff.
- accessing private 3G/4G/5G networks via hotspot from mobiles.

**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.



# Pioneer State High School BYOx Equity Policy

## Rationale

At Pioneer State High School, we are committed to incorporating digital technology into the classroom to support and enhance learning experiences. We recognise that the BYOx program raises a financial cost on students and their families in supplying a device. At the same time, the program can only function if all students have access to appropriate technological resources in all of their classes.

Pioneer State High School takes seriously the role of public education in ensuring all students have access to the same learning outcomes. The purpose of the BYOx Equity Policy is to establish the framework for the BYOx program to provide this for all students, irrespective of their families' financial circumstances.

## Actions

Pioneer SHS will:

- 1) Ensure that device minimum specifications are designed to allow for a range of device options to be considered.
- 2) Assess applications for assistance in meeting the BYOx requirements on a case-by-case basis. Due consideration will be given to all facts including:
  - The level of assistance requested
  - The year level of the student
  - The subjects being studied by the student
  - The technology already available to the student at school and at home
  - Current financial commitments and arrangements with the school
  - Family commitment to the Student Resource Scheme
- 3) Consult with the parent/caregiver to determine what form any assistance will take.

## Students and Parents/Carers:

1. Consider options for the purchase of equipment that meets the minimum device specifications
2. If you believe you are unable to provide a device that meets the minimum specifications and it was made an expectation that your student has a device:
  - The school will liaise with you, your student and their teachers to identify the most appropriate way to address the issue
  - You will be asked to make an agreement with the school that confirms the alternative arrangements made for your student's access to technological resources
3. Pioneer SHS will not purchase a device to assign to your student. Pioneer SHS has limited devices (laptops) it can provide for short-term loan on a School year basis. On approval by the Principal (or delegate), a device will be loaned to your student for the negotiated period.

Return of the device to the Resource Centre/Library is the last day your student will be attending school for 2026 4. You and your student will review and adhere to the rules stipulated on the ICT Responsible Use Agreement Form signed at the time of enrolment and in the current school year.

## **Inappropriate use of equity devices**

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

- Using the device in an unlawful manner
- Intentionally damaging any devices, accessories, peripherals, printers or network equipment
- Leaving the device in a classroom or in the playground
- Losing the device at school
- Not collecting the device at the start of each day
- Not returning the device at the end of each day

## **Misuse, Damage and Loss**

Students should be aware that they are held responsible for their actions while using an equity device. Students will be held responsible for any misuse, damage, loss or theft of an equity device.

Pioneer SHS reserves the right to restrict/remove access of equity devices to ensure the integrity and security of the equity program and the school. The misuse, damage, loss or theft of an equity device may result in disciplinary action as per our Code of Conduct. The misuse, damage, loss or theft of an equity device may also result in a monetary cost to replace the device. This monetary cost will be determined on a case-by-case basis.

<b>Section 1: Student Details</b>			
First Name		Last Name	
School Username		Year Level	
<b>Section 2: Parent Details</b>			
First Name		Last Name	
Address			
Home Phone		Mobile Number	
<b>Section 3: Financial and technology checks</b>			
Does the student have a current ICT Responsible Use Agreement form signed this school year?			Yes/No
Does the student have a signed Student Resource Scheme participation form (at time of enrolment)?			Yes/No
Note: Office staff will verify if the student has the signed forms on file. Application cannot proceed until these forms are completed and signed off.			
Is internet/Wi-Fi available at home?			Yes/No
List all electronic learning devices that are available at home (e.g. home computer, laptop, iPad, tablet etc.).			
<b>Section 4: BYOx Equity Device Application</b>			
Select the period of time your student is applying for an equity device:		Term 1 Term 3	Term 2 Term 4
<b>Section 5: Evidence to Support Application</b>			
<p>• A current Health Care Card or Pensioner Concession card (attach a copy)</p> <p>Parents who may not hold a concession card can discuss directly with the Business Manager for assistance. Your situation will be treated in strict confidence. We may ask you to provide recent evidence to support your application. Your evidence should support your current financial circumstances. Any documents you provide should be dated within four weeks of supplying them. Types of evidence can include the following:</p> <ul style="list-style-type: none"> <li>• official eviction notice (not a warning of possible eviction due to rental arrears)</li> <li>• pending disconnection of essential services, like water, electricity or gas (does not include mobile phone or internet bills)</li> <li>• notice of impending legal action</li> <li>• letter from a charitable organisation regarding loss of employment or inability to provide for basic necessities</li> <li>• bank notice, for example, overdraft call or mortgaged property repossession</li> <li>• overdue medical bills</li> <li>• letter from a doctor verifying the inability to earn an income due to illness or caring for a sick family member</li> <li>• final notice from school regarding payment of mandatory fees</li> <li>• funeral expenses</li> <li>• repossession notice of essential items, like a car or motorcycle. In some cases, these requirements may change, depending on your individual circumstances.</li> </ul>			
<p>I agree to abide by the above rules / the procedure/policy/statement/guideline.</p> <p>Parent / caregiver's name <input type="text"/></p> <p>Signature of parent / caregiver <input type="text"/></p> <p>Date <input type="text"/></p> <p>Student's name <input type="text"/></p> <p>Student's signature <input type="text"/></p> <p>Date <input type="text"/></p>			

*This section is for school use only*

**Section 6: Principal (or delegate) Decision and Notes**

Approved

Not approved

**Section 7: Agreed Period of Equity Device**

The period of time agreed to by the Principal (or delegate), Parent and Student is:

Term 1

Term 2

Term 3

Term 4

Principal's Delegate  
Name

Principal's Delegate  
Signature

Date