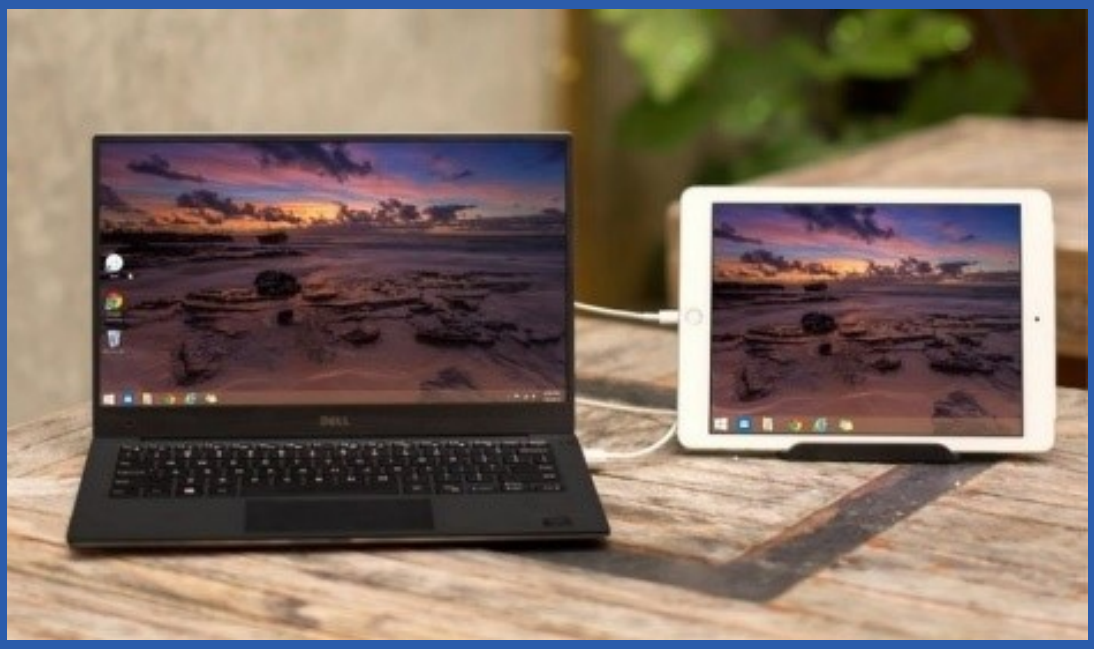
Grand Avenue State School

‘BYOx’ - Bring Your Own Device Charter



A shared commitment to creating a 21st century environment.

Contents

Personally-Owned Mobile Device Charter:

BYOx Overview:

The Bring Your Own 'x' (BYOx) program at Grand Avenue State School is a pathway supporting the delivery of teaching & learning. It 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.

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 mobile devices and their private network accounts.

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

The department has carried out extensive BYOx 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 BYOx model because:

- BYOx recognises 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
- 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.

Need help?

Email: byox@grandavenuess.eq.edu.au
Phone: (07) 3272 0555

Device Selection:

Year 4-6 students will require their device on a daily basis.

We understand choosing the right device for your student is difficult so we have worked with our feeder high schools to create the minimum recommended specifications designed to ensure the device will work well within school environments now and into high school.

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

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

Minimum Device Specifications:

IOS Devices:	Windows Devices:
• iPad 6th Generation • iPad 7th Generation • iPad 8th Generation • iPad Air 2nd Generation • iPad Air 3rd Generation • iPad Air 4th Generation • iPad Pro 2nd Generation • iPad Pro 3rd Generation • iPad Pro 4th Generation • 32BG Storage • Must support 5MHz Wi-Fi	• 4GB RAM • Windows 10 Pro or Home edition • 128GB storage (SSD) • 11" - 15" screen • 6-hour battery life (min) • Must support 5Mhz Wi-Fi

Recommended Device Specifications:

IOS Devices:	Windows Devices:
• iPad 7th or 8th Generation • 128GB storage • Must support 5Mhz Wi-Fi • Protective case • Tempered screen protector	• 8GB RAM • Windows 10 Pro or Home edition • 256GB storage (SSD) • 11" - 15" screen • 6+ hour battery life • Must support 5Mhz Wi-Fi • Laptop case/sleeve

Unsuitable Devices:

iPad Mini, Tablets, Android Devices, Chromebook, and Linux OS devices.

Unsuitable Operating Systems:

Windows RT, Windows 10S, Android and Linux

Device Care:

Your device is your responsibility. Teachers are NOT responsible for the operation, maintenance, or condition of your laptop. Your responsibility as part of the BYOx program is to ensure that each day your device is fully charged, and in a fully functioning order for your school day. Chargers will not be permitted at school.

PLEASE NOTE:

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 minimize 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 Wi-Fi.

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.

Transport to and from school:

- Devices must remain in school bags and protective cases to and from the classroom.
- Students are not permitted to use devices before and after school.

Data Security and Back-ups:

Your data is your responsibility. 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. Students are 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.

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 Information & Communication Technology Acceptable Use Policy.

- 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 username 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' 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.

WARNING:

When outside of the DET network school filtering is not applied. Parent / Carer must ensure they have applied appropriate access and filtering on the device and through their home internet connection. It is the parents' responsibility to ensure students are not accessing inappropriate content at home.

Reporting Requirements:

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.

Students are often worried that if they have accidently seen something inappropriate or had someone strange contact them that they will be in trouble. However, it is important to encourage open and honest communication. Students should feel that they will be supported when sharing something difficult, deemed offensive or explicit. These are opportunities for learning and ensuring safe and responsible digital citizenship.

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 must 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.

Software:

Free Microsoft Office 2016 for students and school staff:

All Queensland state school students can download multiple free copies of the latest Microsoft Office to their personal home computers and mobile devices.

Students will need to use their school email address to sign in.

Your Office subscription lasts for as long as you are a Queensland state school student or school-based staff member.

Visit Microsoft Office Free for Students to download your software.

Norton Antivirus:

Norton Antivirus software is available to All Queensland state school students at a discounted rate. To purchase your Norton Antivirus software, or browse the product pricing and information, please go to The Learning Place, and click the rolling banner ad Norton by Symantec on the top left of the page.

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 DoE network.

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)
- Some school-supplied software e.g. Microsoft Office 365 …
- 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, 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 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, see ACMA CyberSmart)
- Some technical support (please consult Technical support table below)
- Required software, including sufficient anti-virus software
- Complete all software updates at home, including Microsoft operating system updates
- 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	X	X
Device vendor	X	✓ (see specifics of warranty on purchase)	X

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 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 schoolwork.
- 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.
- 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 13.
- Using unsupervised internet chat.
- Sending chain letters or spam email (junk mail).
- Accessing private mobile networks.
- 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. Owners are accountable for their devices and all repairs or replacements are the sole responsibility of the owner and their family.
- 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 BYOx program supports personally-owned mobile devices in terms of access to:

- Internet

However, the school's BYOx 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.

School Contacts:

Below are the contact details regarding ANY information you may require. Please do not hesitate to contact the BYOx team regarding device clarification if you need assistance

Email: byox@grandavenuess.eq.edu.au

Phone: (07) 3272 0555

Frequently Asked Questions:

Question: **Will I need to bring the device to school every day?**
Answer: Yes. Devices are essential tools in each classroom.

Question: **Do I have to buy my child a computer? Is it compulsory?**
Answer: No, the purchase of a computer is not compulsory. The teachers at Grand Avenue State School are keen to use some innovative learning strategies using technology. A 1:1 program (BYOx) cannot be funded by the school, unless we made it for a very small select group of students. We have chosen a more inclusive approach of enabling all students in to bring their own. Children without their own computer will share school owned devices.

Question: **How much time of the day will students spend on their device?**
Answer: The amount of time that students spend on their devices each day will vary on how well the laptop, as a tool for learning, benefits individual students and learning experiences. Some learning experiences will continue to use pen and paper and hands on materials.

Question: **How do I protect my BYOx device?**
Answer: It is the student's responsibility to have their device with them at all times. Protective equipment such as bags or cases need to be organised by the parent and student to keep these devices safe while at school and travelling to and from school. It is the responsibility of the student to look after the device while at school and kept securely in bags.

Question: **Do I need to back up?**
Answer: Yes, it is the student's responsibility at all times to back up all files. The school assessment policy clearly states that loss of data due to technology problems is not an acceptable reason for assessment extensions.

Question: **We already have a device at home; can I use it at school?**
Answer: Yes, hardware and software minimum specifications are provided in this document.

Question: **Will every device work inside the Education Queensland network?**
Answer: No, some devices with low specifications have been found to not connect to the EQ network. These devices may have difficulty with the security filters used by Education Queensland. Please see the device specification list.

Question: **Will the school assist me with network connection settings at school?**
Answer: Limited assistance will be provided. An appointment can be made at the IT Help Desk by individual students for assistance in joining the network.

Question: **Will the school protect the device from virus attacks?**
Answer: Virus protection remains the responsibility of the owner.

Question: **Can I take my BYOx device to IT for repair?**
Answer: The IT Department can perform software repairs on a privately owned device.

Question: **Do I need 3G/4G?**
Answer: Private 3G or 4G services are not to be used at school. The school has an effective wireless network available and it is Education Queensland's policy that whilst at school the school web proxy must be used.

Question: **Does the school provide software for my BYOx device?**
Answer: The Microsoft Office Suite is available free of charge for five student downloads at home. Specialist software required for some subjects will be provided to students enrolled in those courses.

Question: **Will the school assist me with home internet connection settings and issues?**
Answer: No, your home internet provider or local computer technician can assist you with these enquiries.

Question: **Will the teacher be able to provide technical support in class?**
Answer: Limited support in making sure devices are connected to the network.

Question: Can I bring my charger to school?
Answer: The power cord will not be required to be brought to school for health and safety reasons. All chargers are to be left at home. It is the student's responsibility to attend school every day with a fully charged laptop.

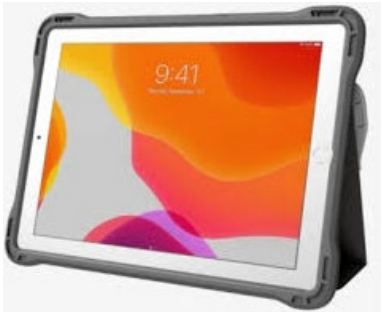
Question: **What is deemed inappropriate?**
Answer: All illegal (unlicensed) software; pirated music or videos; defamatory documents, or images, or any content not suitable for viewing by persons under the age of 18 are deemed inappropriate.

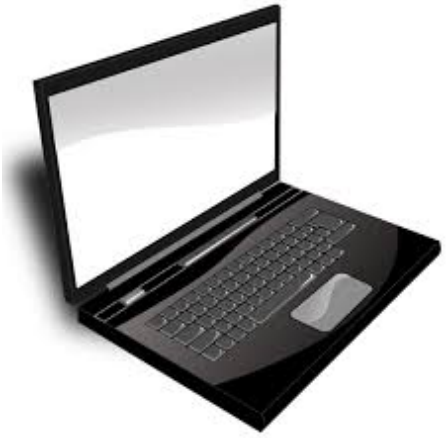
Question: **What happens if the device is damaged at school?**
Answer: If damage is caused by deliberate or careless actions of a student (owner or others), the costs of the repair will be passed onto those involved and necessary behaviour consequences may apply. (NOTE: the school cannot make another family pay for repairs). The device is the owner's responsibility. Adequate insurance taking the above into consideration is highly recommended.

Question: **What happened when my child goes to high school? Will they be able to use their device?**

Answer: We can't speak for all high schools, however students enrolling in our feeder high schools (Forest Lake State High School and Corinda State High School) are supporting the use of laptops with the specs we have recommended.

Please fill in the **BYOx Acceptable Use / Behaviour Agreement & Participation Form** on the next page, detach and **return the one page form to the office as soon as possible**.





BYOx devices CANNOT be brought to school and connected to the EQ network until this agreement is completed in full, signed by parent & student and returned to school.

Grand Avenue State School

BYOx Acceptable Use / Behaviour Agreement and Participation Form

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

☐ I have read the Student BYOx Charter and the Grand Avenue State School Behaviour Management: Responsible Behaviour Plan and I fully understand and agree to comply with all conditions, student obligations and requirements of the program.

☐ I have read, agree to and fully understand the conditions and student and parent / guardian obligations to the ICT Acceptable Use Agreement.

☐ I am aware that non-compliance or irresponsible behaviour in breach of the intent of the BYOx Charter and the Responsible Behaviour Plan, will result in consequences relative to the behaviour.

I …… **from Class** ……
(student name)

will be bringing the following device for the BYOx program:

Make	
Model	
Serial Number	

Student's name: .....
(Please print)

Student's signature: .....**Date:** ……/……. /……..

Parent's/caregiver's name: .....
(Please print)

Parent's/caregiver's signature: .....**Date:** ……/……. /…….