Yeppoon State High School

STUDENT BYOx CHARTER

Contents

CHARTER – Personally owned device charter

BYOx overview

Bring Your Own 'x' (BYOx) 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 devices to access the department's information and communication (ICT) network.

Students and staff are responsible for the security, integrity, insurance and maintenance of their personal 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 devices are used. The 'x' in BYOx represents more than a personally owned device; it also includes software, applications, connectivity or carriage service. Please refer to DET's policy - https://ppr.qed.qld.gov.au/attachment/advice-for-state-schools-on-acceptable-use-of-ict-facilities-and-devices.docx

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, and
- we believe in assisting students to become responsible digital citizens whilst enhancing the teaching and learning processes, and lifting student achievement.

The Australian Curriculum (ACARA) is a priority for our department. Our BYOx program will enable us to embed 21st century learning skills including investigating, creating, communicating, collaborating and operating using ICT's across our curriculum areas.

BYOx will enable daily usage in a variety of formats including digital textbooks, taking photos, note-taking, concept mapping, drafting, planning, report writing, movie making and other multimodal presentations, short formative assessments, polling, discussion boards, email, blogging, online courses, subject specific apps and online testing.

How it will work

The student's personal device will have access to the network through a log-on process that will identify the student as an authorised member of the school community, and ensure the device has the appropriate updated virus protection software. This process will protect both the students and their information contained within the system.

Device selection and minimum specifications

Before acquiring a device to use at school, the parent/carer and student should be aware of the school's specifications for appropriate device type, operating system requirements and software. These specifications relate to enabling diverse class activities, meeting student needs and safe and secure access to the network. Please Note: If your student is likely to study a science subject in Year 11 (Biology, Chemistry, Physics or Marine Studies) then the preferred device is a Laptop.

Device	Minimum	Recommended
Windows Laptop	• Less than 5 Years old Intel i5 or AMD Ryzen • Windows 10 Home (Non S mode) • 13" LCD SCREEN • 8GB RAM • 256GB HDD • Wireless N 5GHz Network card *2.5GHz network cards incompatible with EQ Network*	• Intel i5 6 core 12th Gen (or newer) or Ryzen 5 5600X • Windows 10 or 11 Pro • 15" OLED screen • 8-16GB RAM • 512GB+ SSD Wireless AC 5GHz network card
Apple iPad	• Less than 5 Years old • 8th Gen 10" • iPad OS 16 • 128GB Storage • Protective case • Keyboard or Keyboard case	• 10th or 11th gen • 256GB Storage • iPad OS 17 • Protective Case • Keyboard or Keyboard case
Apple Macbook Pro/Air	• Less than 5 years old • Mac OS 12 (Monterey) • 8GB RAM • 256GB HDD • Wireless N 5GHz Network card *2.5GHz network cards incompatible with EQ Network*	• MacBook Air • M3 Processor • 8-16GB RAM • 512GB SSD • Wireless AC 5GHz network card
Chrome Book	**Incompatible with EQ network. Do not buy.**	
Android Tablets	**Incompatible with EQ network. Do not buy.**	
Regardless of the device chosen, the following are highly recommended: protective case, 5hr battery life, accidental damage, loss & theft insurance, 3 year warranty (for new devices)		

- If these minimum specifications are not met, this device is not supported by DET and may not connect. If you have a device which is very close to the above specifications, please email 2123_byox@.eq.edu.au

The school's BYOx program will support printing, filtered internet access, and file access and storage through the department's network while at school. However, the school's BYOx program does not include school technical support or charging of devices at school. (Students will need to be organised with devices charged.) A FAQ document is available on our school

website.

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. Families should seek advice regarding inclusion of the device in their 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. Similarly, establish the service support available from the supplier.

General precautions:
- Food or drink should not be placed near the device.
- Plugs, cords and cables should be inserted and removed carefully.
- Devices should be carried with the screen closed, and within their protective case.
- Ensure the battery is fully-charged each day.
- Turn the device off before placing it in its bag.

Protecting the screen:
- Avoid poking 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/critical work 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. All files must be scanned using anti-virus software before being downloaded to the department's network. The use of One Drive for storing files is recommended. All students have a school One Drive account.

Students can save data locally to their device for use away from the school network, and should back-up on an external device, such as an external hard drive or USB drive. Students should be aware that service agents may not guarantee the retention of data. The device contents may be deleted and the storage media reformatted during repair.

Use of One Drive will reduce the loss of data through hardware faults.

Acceptable personal device use

Upon enrolment in a Queensland Government school, parental/carer permission is sought to give the student(s) access to the internet, based upon the policy contained within the https://ppr.qed.qld.gov.au/attachment/advice-for-state-schools-on-acceptable-use-of-ict-facilities-and-devices.docx

This policy also forms part of this Student BYOx 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 comply with the department's Code of Conduct (https://ppr.qed.qld.gov.au/attachment/fact-sheet-student-code-of-conduct.pdf) and the Yeppoon State High School 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 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 investigation 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 (eg. a student should not share their username and password with fellow students). Other guidelines are:

- 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/carers 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/carer.

Digital citizenship

Students should be conscious of the content and behaviours they exhibit online and build only a positive online reputation. They should be conscious of the way they portray themselves, the way they treat others online, and know that all interactions and content are easily accessible. This content may form a permanent online record into the future.

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

Parents are required 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 carer promptly.

Students must also seek advice if another user seeks personal information, asks to be contacted, offers gifts by email or asks to meet a student. Students are encouraged to visit https://www.esafety.gov.au/ and to talk/report/learn about cybersafety.

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.

The eSafety Commissioner (https://www.esafety.gov.au/) provides a wealth of resources for educators, parents and students. eSafety is Australia's independent regulator for online safety. They educate Australians about online safety risks and help to remove harmful content such as cyberbullying of children, adult cyber abuse and intimate images or videos shared without consent.

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 conduct and any specific school rules. To help protect students (and staff) from malicious web activity and inappropriate websites, the school operates a comprehensive web filtering system which always applies to all connected devices. 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 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 carers are encouraged to install a local filtering application on the student's device for when they are connected in locations other than school. Parents/carers are responsible for appropriate internet use by

students outside the school. Parents, carers and students are also encouraged to visit the government eSafety website https://www.esafety.gov.au/ for practical advice.

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 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.

Software

Schools may recommend software applications in order to meet the curriculum needs of particular subjects. Parents/carers 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 to another school or graduation.

Monitoring and reporting

Students should be aware that all use of internet and online communication services are auditable and traced to the user's account. 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/associated personal items.

Misuse and breaches of acceptable usage

Students should be aware that they are responsible for their actions while using the internet and online communication services. Students are 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 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 devices may result in disciplinary action that includes, but is not limited to, the withdrawal of access to school supplied services.

Responsible use of BYOx – responsibilities of all stakeholders involved:

➢ the safe and responsible use of facilities/services/resources by students is our goal

School:

- BYOx program induction — including information on (but not responsible for) connection, care of device at school, workplace health and safety, 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 eg. 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 (see https://www.esafety.gov.au/)
- 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 (eg. 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 carers:

- 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/support appropriate digital citizenship & cybersafety (see ACMA CyberSmart)
- 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/carers	✓ (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:

- engaging 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, carers 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 school to enable continuity of learning.
- being courteous, considerate and respectful of others when using a device.
- switching off the device and placing out of sight during class when directed.
- accessing for private use only before or after school, or during "am/pm" breaks
- seeking teacher's approval for use 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
- sending, receiving, displaying or searching or any offensive and anti-social material
- 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 computer networks (eg. the creation, introduction, or spreading of computer viruses, physically abusing hardware, altering source codes or software configurations etc)
- committing plagiarism or violate copyright laws
- using unsupervised internet chat
- sending chain letters or spam email (junk mail)
- accessing private 3G/4G networks during school time
- knowingly downloading viruses/programs capable of breaching the network security
- possessing software that is capable of accessing protected sections of any network, to damage the network or to obtain other users passwords.
- using other users' passwords or allowing others to use your account login
- trespassing in others' folders, work or files
- using any means to avoid scrutiny by teachers of work in progress
- accessing YSHS network locations without appropriate permissions
- 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
- taking in and/or using devices during exams unless instructed 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 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 carers need to be aware that damage to 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.

The BYOx program supports personally owned devices in terms of access to:

- printing
- internet
- file access and storage
- support to connect devices to the school network.

The BYOx program does not support personally owned devices in regard to:

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

Responsible use and Signing of the BYOx Participation Agreement Form:

When PARENTS / CARERS / STUDENTS complete and sign the PARTICIPATION AGREEMENT FORM, this informs the Principal that there is a commitment as follows:

1. I have read and understood the YSHS Student BYOx Charter, the school's Student Code of Conduct and related policies (below)
2. I agree to abide by the expectations outlined in these documents,
3. I am aware that non-compliance or irresponsible behaviour, as per the intent of the YSHS Student BYOx Charter and the Student Code of Conduct and related policies will result in consequences relative to the actual behaviour.

Yeppoon State High School
BYOx PARTICIPATION AGREEMENT

Prior to joining the BYOx program, students need to have returned their Student Resource Scheme form. In addition, if any fees are outstanding, these will need to be paid OR a school approved payment plan is in place.

STUDENTS and PARENTS/CARERS are required to complete and return the PARTICIPATION AGREEMENT to Student Services before the student's device is connected (on-boarded) to the school's computer network.

In signing below, we acknowledge that:

- We accept all policies and guidelines as per the school's Student Code of Conduct, Electronic Devices Policy and Internet Access Agreement.
- We have read and understood the YSHS Student BYOx Charter (included in the enrolment package and published on Yeppoon State High School's website).
- We understand our responsibilities regarding the use of the device and the Internet.
- We accept responsibility for any damage that may occur to the device and have taken relevant steps for insurance.
- We understand that non-compliance or irresponsible behaviour, as per the intent of the YSHS Student BYOx Charter and the school's behaviour policies, will result in relative consequences, which may include exclusion from the school's computer network.
- **We understand that the school's Student Resource Scheme must be paid in advance and the form returned prior to on-boarding the BYOx device or an approved payment plan in place.**

STUDENT'S NAME:	YEAR LEVEL
STUDENT'S SIGNATURE:	
PARENT'S NAME:	
PARENT'S SIGNATURE:	

This form is to be returned to the school office.