Ayr State High School

BYOx Charter

Version 2.3 – 25/08/2023

This type of box indicates a potential solution to the problem.

This type of box indicates problems that you may encounter.

This type of box indicates either a technical explanation, or further actions you may perform to troubleshoot the problem.

Version History

- 1.0 – 23 October 2015 – Initial Version.
- 1.1 – 28 October 2015 – Refined Permission form.
- 1.2 – 26 November 2015 – Amended section detailing support to make clear that some support is limited on iOS/Android devices.
- 1.3 – 08 February 2016 – Amended dates on documents.
- 1.4 – 29 November 2016 – Amended dates on documents.
- 1.5 – 29 January 2018 – Amended dates on documents, rebranded DETE to DoE, modified links to Cybersafety Help Button as it is now under the umbrella of the Office of the eSafety Commissioner.
- 1.6 – 5 February 2018 – Amended link to PPR Policy regarding Acceptable Use of ICT's
- 1.7 – 18 February 2019 – Amended dates on document – added new logo.
- 1.8 – 5 December 2019 – Updated for 2020.
- 1.9 – 4 February 2021 – Updated for 2021.
- 2.0 – 21 February 2022 – Updated for 2022.
- 2.1 – 22 February 2022 – Updated to include windows 11
- 2.2 – 30 February 2023 – Updated for 2023 and included Mac versions
- 2.3 – 25 August 2023 – Updated for 2024; renamed Responsible Behaviour Plan to Student Code of Conduct

Purpose of Document

This document details terms and conditions regarding student participation in the school's BYOx program, and outlines each particular stakeholder's responsibilities.

Personally-owned mobile 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 mobile devices to access the department's information and communication technology (ICT) network.

These mobile devices include but are not limited to laptops, tablet devices, voice recording devices (whether or not integrated with a mobile phone or MP3 player), game devices (eg PSPs, Game Boys), USBs, DVDs, CDs and smart phones. 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 - see 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 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
- the program assists students to become responsible digital citizens which enhances the teaching and learning process and enables students to develop skills and engage in 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, operating system requirements and software. These specifications relate to the suitability of the device to enable class activities, meet student needs and promote safe and secure access to the department's network. Current guidelines are available on the school's website.

The school's BYOx program will support printing, filtered internet access, and file access and storage through the department's network while at school. The school's BYOx program has limited school technical support and encourages charging of devices to occur at home.

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 a home and contents insurance policy. To assist, Ayr SHS has a number of lockers available for storage during school hours.

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
- 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
- Avoid 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 will 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. It is advised that an external back-up device be used, 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 Acceptable Use of the Department's Information, Communication and Technology (ICT) Network and Systems

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 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 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 (ie 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 of the content they create 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 Student Code of Conduct 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 resources on the website of the Office of the eSafety Commissioner to seek support and learn about a range of cybersafety issues, and can report cyberbullying using the button on their desktop.

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 Stand Out From the Crowd Action Plan.

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 Student Code of Conduct. 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 Department of Education and Training 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 eSafety Commissioner's 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

The School will install a range of software 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

- deliver 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
- provide network connection at school
- provide internet filtering (when connected via the school's computer network)
- provide access to some technical support (please consult technical support table below)
- provide some school-supplied software eg Adobe, Microsoft Office 365
- provide printing facilities at school
- confirm BYOx Charter Agreement and facilitate access to network

Student

- participate in BYOx program induction
- acknowledge that core purpose of device at school is for educational purposes
- implement appropriate care of device
- demonstrate appropriate digital citizenship and online safety (for more details, see eSafety Comissioner's website)
- ensure 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 (ie a student should not share their username and password with fellow students)
- access technical support as required (please consult technical support table below)
- maintain a current back-up of data
- charge device at home
- abide by intellectual property and copyright laws (including software/media piracy)
- abide by internet filtering (when not connected to the school's network)
- ensure personal login account will not be shared with another student, and device will not be shared with another student for any reason
- understand and sign the BYOx Charter Agreement

Parents and caregivers

- participate in BYOx program induction
- acknowledge that core purpose of device at school is for educational purposes
- ensure that student/s bring their laptop to school each day
- implement internet filtering (when not connected to the school's network)
- encourage and support appropriate digital citizenship and cybersafety with students (for more details, see eSafety Comissioner's website)
- access technical support as required (please consult technical support table below)
- provide required software, including sufficient anti-virus software
- purchase protective backpack or case for the device
- ensure adequate warranty and insurance of the device
- understand and sign 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, encyclopedias, etc.
  - researching and learning through the school's eLearning environment
- Ensure 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 Student Code of Conduct.
- 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:

- printing (except for Android/iOS Devices where this is not possible natively)
- internet
- file access and storage (except for Android/iOS devices where this is not possible natively)
- support to connect devices to the school network

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

Accessing BYOx Services

1	Collect BYOx Charter and Agreement from office
2	Read Charter document and return signed A4 Agreement to office
3	Enrol student BYOx device into Intune (preferably at home – please see below)
4	Seek advice from School ICT Support Officer if required

BYOxLink Getting your child's device ready for school
The Department of Education is implementing a new Bring Your Own (BYO) device solution called "BYOxLink" that enables students to use their privately owned devices to access school email, learning applications, printers and shared network drives at the school. Enrolment in the BYOx system is managed via **Microsoft inTune**. Links to support videos to complete this enrolment can be found on the school's website.

What does "enrolling your child's device into Intune", mean for my child?
Enrolling your child's device into Intune, will mean your child will be able to:

- access the school Wi-Fi network and have school email automatically set up and configured
- access the school's learning applications and websites
- self-manage their personal device

What if I am having trouble with the enrolment?
If you are having trouble or have further questions, contact your school IT support or school administration staff. Please note, your child will need to stay logged in for up to 15 minutes after enrolment is done, to make sure all Intune set-up is complete. Enrolment of a device may take 10-15 minutes.

Where is it best to enrol my child's device into Intune?
We recommend that your child enrols their device into Intune at home using the home Wi-Fi internet connection. If needed, your child may also enrol at school, using the school guest Wi-Fi service, EQGUEST.

How much home internet data allowance does Intune use?
A small amount of data is required to both enrol your child's device into Intune and subsequently to use Intune at home to access school email and learning applications. Home data allowance will be required if your child is accessing websites and school applications; the amount depends on the applications.

What can school administration staff see or not see on my child's device?

What the school administration (Intune) can see on the device

Your school can only see information that is relevant to the school:
a. Device owner.
b. Device name.
c. Device model.
d. Device manufacturer.
e. Operating system and version eg: iOS 13, Windows 10 or Windows 11
f. App inventory and App names, like Microsoft Office 365 (the school can only see school managed Apps).
h. Device serial number and IMEI.

What the school administration (Intune) cannot see on the device

Your school does not monitor student's use of the device
a. Cannot see your child's personal information.
b. Cannot see what your child is doing on their device.
c. Does not track student's locations/device location.
d. Does not provide information on personally installed applications.
e. Home Network cannot be seen.
f. Calling and web browsing history.
g. Email and text messages.
h. Contacts.
i. Calendars.
j. Passwords.
k. Pictures, including what's in the photos app or camera roll.
l. Files.

Student BYOx Charter Agreement

The Student BYOx Charter agreement form must be signed and returned to the school before any device owned by the student will be authorised to connect to the school network.

The student and parent/caregiver must carefully read the charter before signing it. Any questions should be addressed to the school and clarification obtained before signing.

In signing below, we acknowledge that we,

- accept all policies/guidelines as per the Student Code of Conduct and conditions detailed in the Student BYOx Charter.
- understand my responsibilities regarding the use of the device and the internet
- understand that failure to comply, or irresponsible behaviour as outlined in the Student BYOx Charter and Student Code of Conduct will result in consequences relative to the behaviour (eg: suspension of the student's ability to connect to the school network on all personally owned devices).
- understand that I must bring my personal device to school, fully charged, on a regular basis.
- understand that the school is not liable in any way for damage to my personal device
- understand that my access to other digital devices in the school may be limited
- understand that students must not photograph, record, film any students or school personnel with their personal devices without the express permission of the individuals concerned **and** the supervising teacher.
- understand that damage to personal devices owned by other students or staff may result in significant consequences in relation to breaches of the school's Student Code of Conduct
- understand that data must be effectively managed by backing up classwork and assessment to the school server on a regular basis (H Drive)

After reviewing and understanding the responsibilities outlined in the *Acceptable Personal Mobile Device Use* section above and relevant documents, we:

☐ **agree** to the provision of access for my students personally owned device to the school's network.

☐ do not agree to the provision of access for my students personally owned device to the school's network.

Student's name	**Signature of student**	**Date**
Parent / caregiver's name	**Signature of parent / caregiver**	**Date**
Designated school representative's name	**Signature of school representative**	**Date**

Office Use Only

Student Username		**Current Year Level**	
Device Requirements Check		**Date BYO Group Added on Server**	