CALLIOPE STATE HIGH SCHOOL

Student BYOx Charter 2026

To create a community of agile learners who are thinkers, resilient and kind.

CONTENTS

PERSONALLY-OWNED MOBILE DEVICE CHARTER

BYOx Overview

Bring Your Own Device (BYOx) is a pathway supporting the delivery of 21st century learning. It is a term used to describe a digital device ownership model where students use their personally-owned device to access the department's information and communication (ICT) network.

Students 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. At CSHS, digital devices specifically excludes mobile phones per our Student Code of Conduct.

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.
- Our BYOx program assists 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.

For further information on BYOx please visit our BYOx Program page on our website: https://calliopeshs.eq.edu.au/curriculum/bring-your-own-device

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 ensure that the device is suitable for classroom activities, meets student learning needs, and supports safe and secure access to the department's network.

Minimum device specification at Calliope State High School are listed below:

SPECIFICATION	DETAIL
Processor	Intel 8th Generation i3
RAM	8GB
Screen Size	13"
Storage	256GB SSD
Operating System	Windows 11 Home or Professional Edition
Wireless	802.11ac adaptor - capable of connecting to a 5GHz network
Ports	At least one USB port, audio in/out to connect wired headphones.
Battery Life	Minimum 6 hours of continual use
Anti-virus	Windows built-in Microsoft Defender Antivirus is adequate.
Damage Protection	A quality semi-hard or hard laptop case is recommended. Soft Neoprene sleeves don't provide adequate protection. Accidental damage protection insurance is advised.
Not Supported	**Copilot+ PC running on Snapdragon ARM processor, Google ChromeOS (Chromebook), Apple MacOS (MacBook), Linux (all versions) & Android.**

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.

Students are to keep their laptop with them at all times to ensure its safety as part of the BYOx Agreement. School staff will not store or hold onto student laptops.

Malicious damage will be investigated by the school as part of our Student Code of Conduct, however liability remains with the laptop owner.

General precautions

- Food or drink should never be placed near the device.
- Plugs, cords and cables should be inserted and removed carefully.
- Devices should be carried within their protective case where appropriate.
- Carrying devices with the screen open should be avoided.
- Ensure the battery is fully charged each day.
- Turn the device off before placing it in its bag.

Protecting the screen

- Avoid poking at the screen — even a touch screen only requires a light touch.
- Don’t place pressure on the lid of the device when it is closed.
- Avoid placing anything on the keyboard before closing the lid.
- Avoid placing anything in the carry case that could press against the cover.
- Only clean the screen with a clean, soft, dry cloth or an anti-static cloth.
- Don’t clean the screen with a household cleaning product.

Data Security and Back-ups

The student is responsible for the backup of all data therefore students must ensure they have a process of backing up data securely, reliably and regularly. Otherwise, should a hardware or software fault occur, assignments and the products of other class activities may be lost.

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. Hardware or software faults will not be accepted as a reasonable excuse for not completing or submitting assessment tasks on time.

Students have a variety of methods available to ensure their data is backed up. While at school, students may be able to save data to the school's network, which is safeguarded by a scheduled backup solution. By logging into Microsoft OneDrive for Business using their school account, students can save and sync their school files to the cloud. External USB drives can also be used for backing up files.

Warranty, Repairs and Maintenance

Laptop repairs and maintenance are the responsibility of the laptop owner. Swift turnaround times associated with maintenance and repair are essential.

Having a good understanding of your laptop warranty and what is covered is highly recommended.

School staff will not troubleshoot or repair student devices other than to connect the device to the school network and printing services.

Charging of Devices

Student laptops are to be fully charged at home and have the capacity to last the entire school day.

Students do have the ability to charge their devices during class at limited charging stations within the classrooms.

Printing

Papercut will be installed on each students' laptop as part of the network on boarding process. Papercut allows the school to manage the quantity of printing each student can perform at the school. Each student will receive a printing allocation per year and should this amount be exceeded families are able to purchase additional printing allocation through QKR!

Connecting to the CSHS Network

Calliope State High School deploys a BYOxLink platform that allows students to connect their personal laptop to the schools' network.

To establish a new laptop connection to our network, students need to undertake a series of steps via a system called Microsoft Intune. This connection process must be completed at home.

Microsoft Intune is a mobile device management platform that will also assist your child in being 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

Mobile/Personal Hotspots and VPN's

Using mobile and personal hotspots or inbuilt data connectivity via a SIM card or use of a VPN (Virtual Private Network), can provide students with UNFILTERED Internet connections within the school grounds. These types of internet connections need to be disabled before arrival at school, as the school cannot monitor or take responsibly for content accessed via these methods.

School Technical Support

Calliope State High School employs a full-time Technical Officer, who is available daily between 9.00am and 3.00pm at the BYOx Help Desk to support students with BYOx connection and installation issues.

School Technical Officers are only able to provide a limited level of support for BYOx devices. This support includes:

- ✓ Connection of the laptop to the school network
- ✓ Connection of the device to the school printers
- ✓ Installation of optional school software

School Technical Officers are <u>not</u> able to support students with (but not limited to):

- × Hardware faults
- × Windows software issues
- × Physical damage to your device
- × Issues caused by viruses

ACCEPTABLE PERSONAL MOBILE DEVICE USE

Upon enrolment in a Queensland Government school, parental or caregiver permission is sought to give the student(s) access to the internet, based upon the policy contained within the Acceptable Use of the Department's Information, Communication and Technology (ICT) Network and Systems.

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

Communication through internet and online communication services must also comply with the CSHS Student Code of Conduct available on the school website.

While on the school network, students <u>should not</u>:

- 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
- install or use a VPN (Virtual Private Network) to bypass Internet filtering
- 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 complex 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. The password should be changed 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. To ensure no one else can use their device, students should lock or sign out of their device at the end of each session and when away from their 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 Student Code of Conduct also supports students by providing school related expectations, guidelines and consequences.

Bullying and cyberbullying - preventing and responding

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 esafety to learn about online safety risks.

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 CSHS Student Code of Conduct 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 or parent/carer'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)
- some technical support
- some 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 complex 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
- 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
- required software
- protective backpack or case for the device
- adequate warranty and insurance of the device
- understanding and signing the BYOx Charter Agreement.

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

- Use BYOx 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 BYOx device.
- Switch off and place BYOx device out of sight 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 BYOx 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 personal hotspot during lesson time
- knowingly downloading viruses or any other programs capable of breaching the department's network security
- using a VPN on the department network to bypass Internet filtering
- 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.