BYOx Responsible Use Guidelines 2025

CLERMONT STATE HIGH SCHOOL

Clermont State High School
1 KITCHENER ST, CLERMONT QLD 4721 | Ph. (07) 4983 4333 | www.clermontshs.eq.edu.au

Table of Contents

BYOx overview

Clermont State High encourages students to participate in our Bring Your Own Device 'x' (BYOx) program to support the delivery of 21st century learning to students. This document defines the acceptable and responsible use guidelines for our BYOx program.

BYOx is a term used to describe a digital device ownership model where students use their personally-owned devices to access the Department of Education (DoE) Information and Communication Technologies (ICT) network.

These devices include laptops and tablets, not mobile phones. Access to the DoE ICT network is provided only if the device meets the DoE security requirements which, at a minimum, requires that anti-virus software has been installed, is running and is kept updated on the device.

Students are responsible for the security, integrity, insurance and maintenance of their personal devices and their private network accounts.

Clermont SHS has chosen to implement the BYOx model because:

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

Students who are not able to bring their own device, will be able to loan a school laptop for daily use. The same standard of device care is expected of these devices.

Device selection

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

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

The minimum specifications of the device can be found below.

Minimum Specifications

When purchasing a laptop for your student or deciding if one from home will be adequate, please ensure you consult the BYOx Minimum Device Specifications.

These specifications relate to the suitability of the device in enabling class activities, meeting student needs and promoting safe and secure access to the Department of Education network.

Windows 10/11 Laptop preferred.

Specification	**Detail**
Processor	Intel 8th Generation i3
RAM	8GB or higher
Screen Size	No less than 9.7 inches
Storage	256GB SSD
Operating System	Windows 11 Home, Professional, Education or SE Edition
Wireless	Must be capable of connecting to a 5GHz network
Ports	At least one USB port
Battery life	Minimum 6 hours of continual use
Anti-virus	Recommended
Damage Protection	A protective case and accidental damage protection are recommended
These devices are Not Supported	• Android devices • Google Chromebooks • Linux Devices • iPad

Students will need local admin access to their BYOx machine for the initial on-boarding (connecting). They will also need any software that has been installed to limit their access turned off/removed for the connection to be successful.

Should you choose to purchase or provide your student with a device that does not meet the above requirements your student may encounter the below issues:

- The device may not operate with our networks
- The device may take your student longer to open, close, and use applications
- The device may not allow your student to access applications
- The device may mean your student will spend their break time charging their laptop during as no charging of laptops is permitted in classrooms

This list is not exhaustive but all or any of the above have potential to impact your students' learning.

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 BEFORE arriving at school.
- Turn the device off before placing it in its bag.

Protecting the screen

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

Data security and back-ups

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

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

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

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

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

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 not have the ability to charge their devices during class and only limited charging opportunities may be available during breaks.

Connecting to the school network

Clermont State High School deploys a BYOxLink platform that allows students to connect their personal laptop to the DoE 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

Acceptable personal device use

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

This policy is part of the Clermont State High School acceptable-use conditions 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 DoE Student Code of Conduct available on our school website.

While on the school network, students should not:

- create, participate in or circulate content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disable settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
- use unauthorised programs and intentionally download unauthorised software, graphics, music or videos
- intentionally damage or disable computers, computer systems, school or government networks
- use the device for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

Note: Students' use of internet and online communication services may be audited at the request of appropriate authorities for investigative purposes surrounding inappropriate use.

Passwords

Use of the school's ICT network is secured with a user name and password. The password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g. a student should not share their username and password with fellow students).

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 Student Code of Conduct also supports students by providing school related expectations, guidelines and consequences.

Cybersafety

The Department of Education supports every child and young person in Queensland state schools to learn and engage safely in the digital world. With the rise of technology and increasing access for young people, Online Safety in Queensland State Schools (PDF, 4 MB) document provides guidance on how the department responds and supports schools, students, parents and the community, in keeping young people safe online.

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 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 information 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 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 DoE network must also be reported to the school.

The personally-owned devices have access to home and other out of school internet services and those services may not include any internet filtering. Parents and caregivers are encouraged to install a local filtering application on the student's device for when they are connected in locations other than school. Parents/caregivers are responsible for appropriate internet use by students outside the school.

Parents, caregivers and students are also encouraged to visit the website of the Australian eSafety Commissioner for resources and practical advice to help young people safely enjoy the online world.

Privacy and confidentiality

Students must not use another student or staff member's username or password to access the school network or another student's device, including not trespassing in another person's files, home drive, email or accessing unauthorised network drives or systems.

Additionally, students should not divulge personal information via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school. It is important that students do not publish or disclose the email address of a staff member or student without that person's explicit permission. Students should also not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. They should ensure that privacy and confidentiality is always maintained.

Intellectual property and copyright

Students should never plagiarise information and should observe appropriate copyright clearance, including acknowledging the original author or source of any information, images, audio etc. used. It is also important that the student obtain all appropriate permissions before electronically publishing other people's works or drawings. The creator or author of any material published should always be acknowledged. Material being published on the internet or intranet must have the approval of the principal or their delegate and have appropriate copyright clearance.

Copying of software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.

Software

Schools may recommend software applications in order to meet the curriculum needs of particular subjects. Parents/caregivers may be required to install and support the appropriate use of the software in accordance with guidelines provided by the school. This includes the understanding that software may need to be removed from the device upon the cancellation of student enrolment, transfer or graduation.

Monitoring and reporting

Students should be aware that all use of internet and online communication services can be audited and traced to the account of the user.

All material on the device is subject to audit by authorised school staff. If at any stage there is a police request, the school may be required to provide the authorities with access to the device and personal holdings associated with its use.

Misuse and breaches of acceptable usage

Students should be aware that they are held responsible for their actions while using the internet and online communication services. Students will be held responsible for any breaches caused by other person(s) knowingly using their account to access internet and online communication services.

The school reserves the right to restrict/remove access of personally owned mobile devices to the intranet, internet, email or other network facilities to ensure the integrity and security of the network and to provide a safe working and learning environment for all network users. The misuse of personally owned mobile devices may result in disciplinary action which includes, but is not limited to, the withdrawal of access to school supplied services.

Responsible use of BYOx

Our goal is to ensure the safe and responsible use of facilities, services and resources available to students through the provision of clear guidelines.

Responsibilities of stakeholders involved in the BYOx program

School

BYOx program induction — including information on (but not responsible for) connection, care of device at school, workplace health and safety, appropriate digital citizenship and cybersafety

- network connection at school
- internet filtering (when connected via the school's computer network)
- limited technical support (please consult Technical support table below)
- limited school-supplied software e.g. Adobe, Microsoft Office 365
- printing facilities
- school representative signing of BYOx Charter Agreement.

Student

- participation in BYOx program induction
- acknowledgement that core purpose of device at school is for educational purposes
- care of device
- appropriate digital citizenship and online safety (for more details, visit the website of the Australian eSafety Commissioner)
- security and password protection — password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g. a student should not share their username and password with fellow students)
- some technical support (please consult Technical support table below)
- maintaining a current back-up of data
- charging of device
- abiding by intellectual property and copyright laws (including software/media piracy)
- internet filtering (when not connected to the school's network)
- ensuring personal login account will not be shared with another student, and device will not be shared with another student for any reason
- understanding and signing the BYOx Charter Agreement.

Parents and caregivers

- participation in BYOx program induction
- acknowledgement that core purpose of device at school is for educational purposes
- internet filtering (when not connected to the school's network)
- encourage and support appropriate digital citizenship and cybersafety with students (for more details, visit the website of the Australian eSafety Commissioner)
- some technical support (please consult Technical support table below)
- required software, including sufficient anti-virus software
- protective backpack or case for the device
- adequate warranty and insurance of the device
- understanding and signing the BYOx Charter Agreement.

Technical support

	Connection:	Hardware:	Software:
Parents and Caregivers	✓ (home-provided internet connection)	✓	✓
Students	✓	✓	✓
School	✓ school provided internet connection	(dependent on school-based hardware arrangements)	✓ (some school-based software arrangements)
Device vendor		✓ (see specifics of warranty on purchase)	

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

Use mobile devices for:

- engagement in class work and assignments set by teachers
- developing appropriate 21st Century knowledge, skills and behaviours
- authoring text, artwork, audio and visual material for publication on the Intranet or Internet for educational purposes as supervised and approved by school staff
- conducting general research for school activities and projects
- communicating or collaborating with other students, teachers, parents, caregivers or experts as part of assigned school work
- accessing online references such as dictionaries, encyclopaedias, etc.
- researching and learning through the school's eLearning environment
- ensuring the device is fully charged before bringing it to school to enable continuity of learning.
- be courteous, considerate and respectful of others when using a mobile device.

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

- using the device in an unlawful manner
- creating, participating in or circulating content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disabling settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
- downloading (or using unauthorised software for), distributing or publishing of offensive messages or pictures
- bypassing the schools filtering service
- using obscene, inflammatory, racist, discriminatory or derogatory language
- using language and/or threats of violence that may amount to bullying and/or harassment, or even stalking
- insulting, harassing or attacking others or using obscene or abusive language
- deliberately wasting printing and Internet resources

- intentionally damaging any devices, accessories, peripherals, printers or network equipment
- committing plagiarism or violate copyright laws
- using unsupervised internet chat
- sending chain letters or spam email (junk mail)
- accessing private 3G/4G/5G networks.
- accessing private 3G/4G/5G networks via hotspot from mobiles.
- knowingly downloading viruses or any other programs capable of breaching the department's network security
- using the device's camera anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets
- invading someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material
- using the device (including those with Bluetooth functionality) to cheat during exams or assessments.
- take into or use devices at exams or during class assessment unless expressly permitted by school staff.

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
- internet
- file access and storage
- 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.

Loan Equipment

Clermont State High School will provide access to a loan device (windows laptop) should your student not be able to bring their own device to school. This device will meet our schools' minimum device specifications. The school has a variety of laptops that will be available for loan.

Each device will be:

- able to be connected to the school network and have filtered internet and email.
- available for loan and use during the school day only
- installed with DoE standard suite of productivity software.

Responsible use agreement

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

- We have read and understood the BYOx Responsible Use Guidelines and the school Student Code of Conduct
- We agree to abide by the guidelines outlined by the school
- We are aware that non-compliance or irresponsible behaviour, as per the intent of the BYOx Responsible Use Guidelines and the Student Code of Conduct, will result in consequences relative to the behaviour.

Student's name:		**ID No:**	
	(Please print)	**Year:**	
Student's signature:		**Date:**	**/ /**
Parent/Caregiver's name:			
	(Please print)		
Parent/Caregiver's signature:		**Date:**	**/ /**