



Student BYOx

Murgon State High School



Great state. Great opportunity.



Contents

BYOx Overview	3
Device information and advice.....	4
Device selection.....	4
IMPORTANT NOTES.....	4
Device care	5
General precautions	5
Protecting the screen	5
Data security and back-ups	5
Acceptable personal mobile device use	6
Passwords.....	6
Digital citizenship.....	7
Cyber safety.....	7
Students must never initiate or knowingly forward emails, or other online content, containing	7
Students must never send, post, or publish.....	7
Web filtering.....	8
Privacy and confidentiality	8
Intellectual property and copyright.....	9
Software	9
Monitoring and reporting.....	9
Misuse and breaches of acceptable usage	9
Responsible use of MSHS BYOx Learning devices	10
Responsibilities of stakeholders involved in the program.....	10
School	10
Student	10
Parents and caregivers	10
Technical Support.....	11
The following are examples of responsible use of devices by students.....	11
The following are examples of irresponsible use of devices by students.....	12
In addition to this	13
How to guide	14

BYOx Overview

Bring Your Own 'x' (BYOx) program at Murgon State High School 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 (ICT) network.

These mobile devices include Windows and Apple Devices. 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 parents are responsible for the security, integrity, insurance and maintenance of their personal mobile devices and their private network accounts.

The BYOx acronym is used by the department and 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 conducted extensive BYOx research within Queensland state schools. The research was 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 acknowledges the demand for seamless movement between school, work, home, and play
- Our BYOx program assists students to improve their learning outcomes in a contemporary educational setting
- assisting students to become responsible digital citizens enhances the teaching learning process and achievement of student outcomes as well as the skills and experiences that will prepare them for their future studies and careers.

Device information and advice

Device selection

Before acquiring a device to use at school you 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 enabling class activities, meeting student needs, and promoting safe and secure access to the department's network.

Windows

Specifications	
Processor Minimum	Intel i5 / AMD Ryzen 5
Memory Minimum (RAM)	16GB
Disk Minimum Solid State Drive only (SSD)	256GB to 512GB
Display	12 to 14"
Graphics	Integrated
Warranty	3-4 years onsite

Apple Mac

Specifications	
Processor Minimum	Macbook Air M3 or later
Memory Minimum (RAM)	8GB
Disk Minimum Solid State Drive only (SSD)	256GB
Display	13 or 15"
Warranty	3-4 years onsite

IMPORTANT NOTES:

- For students studying design or technology subjects.
For Example: Digital Technologies, Digital Arts, ITD.
intel i5 CPU and 16GB Ram are essential.
- Windows 10 - Windows R/T – Windows S Mode, Android, Chromebook, and ATOM/Celeron devices are **NOT** supported.
- Protective case/bag is highly recommended
- Antivirus software suite is optional on Windows 11 as this comes with Windows Defender, which will be sufficient, If the device is an Apple Laptop antivirus will need to be purchased and installed.

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 no school technical support and requires battery charging of devices to occur at home. For this to be successful the device must support a full day's use. 4-6 hours.

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 inclusions in home and contents insurance policy.

It is advised that 'accidental damage' and 'warranty' policies are discussed at point of purchase to minimise the 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.
- Devices should be put in *sleep* or *hibernate* mode before moving around.
- Ensure the battery is fully charged each day before/after attending school.

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 use of OneDrive is allowed for this. Please note that access to OneDrive is conditional in being an enrolled student in an Education Queensland School.

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. 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, USB or OneDrive.

Students should also be aware that if 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 as part of the repair process.

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 Charter. The acceptable-use conditions apply to the use of the device and Internet both on and off school grounds.

Communication through Internet and online communication services must also comply with the department's [Code of School Behaviour](#) and the school's behaviour policies.

While on the school network, students should not:

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

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

Passwords

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

The password should be changed regularly, as well as when prompted by the department or when known by another user.

Personal accounts are not to be shared. Students should not allow others to use their personal account for any reason.

Students should log off at the end of each session to ensure no one else can use their account or device.

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.

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 behaviour policies also support students by providing school related expectations, guidelines and consequences.

Cyber Safety

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 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 and Guardians are encouraged to explore online resources 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 can damage the recipient's computer
- chain letters, hoax emails or phishing emails
- spam (such as unsolicited advertising)

Students must never send, post, or publish:

- inappropriate or unlawful content, which is offensive, abusive, or discriminatory
- threats, bullying or harassment of another person
- sexually explicit or sexually suggestive content or correspondence
- false or defamatory information about a person or organisation.

Parents, caregivers and students are encouraged to read the department's [Cybersafety and Cyberbullying guide for parents and caregivers](#).

Web filtering

The Internet has become a powerful tool for teaching and learning. However, students need to be careful and vigilant regarding some web content. At all times students, while using ICT facilities and devices, will be required to act in line with the requirements of the [Code of School Behaviour](#) and any specific rules of the school. To help protect students (and staff) from malicious web activity and inappropriate websites, the school operates a comprehensive web filtering system. Any device connected to the Internet through the school network will have filtering applied.

The filtering system provides a layer of protection to staff and students against:

- inappropriate web pages
- Spyware and malware
- peer-to-peer sessions
- scams and identity theft

This purpose-built web filtering solution takes a precautionary approach to blocking websites including those that do not disclose information about their purpose and content. The school's filtering approach represents global best-practice in Internet protection measures. However, despite internal departmental controls to manage content on the Internet, illegal, dangerous, or offensive information may be accessed or accidentally displayed. Teachers will always exercise their duty of care but avoiding or reducing access to harmful information also requires responsible use by the student. 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 DETE 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](#) 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 obtains 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 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 to meet the curriculum needs of 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 people knowingly using their account to access Internet and online communication services.

The school reserves the right to restrict/remove access of personally owned mobile computer 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 MSHS BYOx Learning devices

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

Student

- Student participation in BYOX program induction
- acknowledgement that core purpose of device at school is for educational purposes
- care of device
- appropriate digital citizenship and online safety (for more details, see [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)
- maintaining a current back-up of data
- charging of device
- abiding by intellectual property and copyright laws (including software/media piracy)
- Internet filtering (when not connected to the school's network)
- ensuring personal login account will not be shared with another student, and device will not be shared with another student for any reason
- understanding and signing the BYOx Charter Agreement.

Parents and caregivers

- participation in BYOx program induction
- acknowledgement that core purpose of device at school is for educational purposes
- Internet filtering (when not connected to the school's network)
- encourage and support appropriate digital citizenship and Cybersafety with students (for more details, see [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

	Internet Connection:	Hardware:	Software:
Parents and Caregivers	✓ (home)	✓	✓
Students	✓	✓	✓
School	✓ (school)	✓ (hands off, diagnosis and trouble-shooting)	✓ (school-based software arrangements)
Device vendor		✓ (ADP – Accidental Damage Protection - Manufacturer and Extended Warranties)	

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 schoolwork
 - accessing online references such as dictionaries, encyclopedias, etc.
 - researching and learning through the school's eLearning environment
 - ensuring the device is fully charged before bringing it to school to enable continuity of learning.
- Be courteous, considerate, and respectful of others when using a mobile device.
- Switch off and place out of sight the mobile device during classes, where these devices are not being used in a teacher directed activity to enhance learning.
- Use the personal mobile device for private use before or after school, or during recess and lunch breaks.
- Seek a teacher's approval where they wish to use a mobile device under exceptional 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), 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 violating copyright laws
- using unsupervised Internet chat
- sending chain letters or spam email (junk mail)
- accessing private 3G/4G/5G 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 being 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 behaviour policies.
- 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 regarding:

- technical support other than connection to the school network
- charging of devices at school (**personal charging bricks and chargers or leads are not permitted at school**)
- security, integrity, insurance and maintenance of personal accounts and software.

Murgon State High School offers a 'Bring Your Own Device' program. Our school network supports Windows 11 devices, iPads and MacOS.

Please read through this Student BYOx charter document and use the support documents provided in the link below to assist with onboarding your device onto our school network.

<https://murgonshs.eq.edu.au/curriculum/bring-your-own-device>