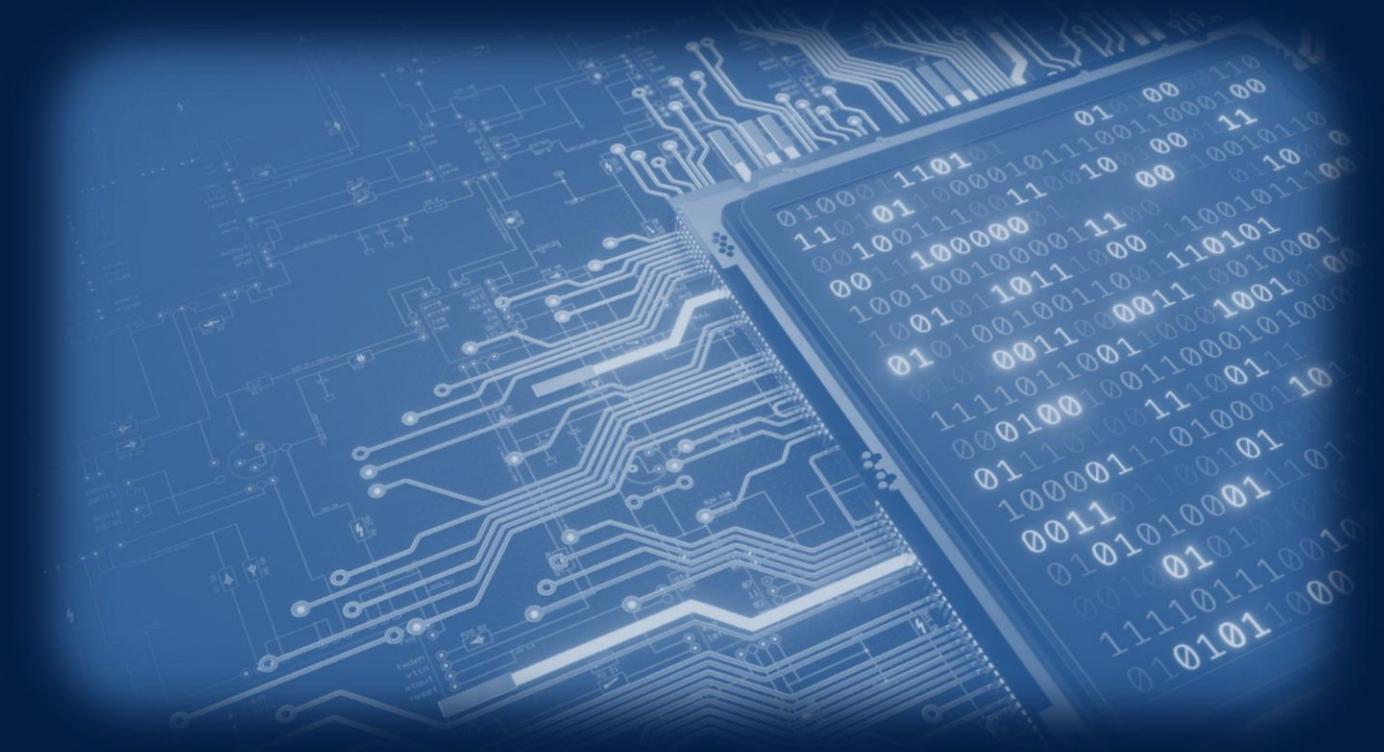
Mitchelton State High School



BYO Student Handbook
2026

Document Version – **2025.2**

Introduction

Starting in 2026 the BYO (Bring Your Own) program at Mitchelton State High School enables students to bring personally owned devices to school to support their learning. This handbook outlines the expectations, responsibilities, and requirements for participation in the program to ensure a safe, secure, and productive digital learning environment. This program is initially for Year 7, 8, 10 and 11 and will roll out to all year levels in 2027 as our existing device program concludes.

Program objectives

- Enhance student learning through access to digital tools.
- Promote responsible digital citizenship.
- Support seamless learning between school and home.
- Ensure safe and secure use of personal devices on the school network.

What are families required to provide?

- A device that meets the minimum hardware and software specifications as outlined in the minimum device specifications fact sheet found on our website.
- The program is specifically limited to **laptops**. Other devices such as **tablets, smartphones, and peripheral mobile devices** are not supported under this program.
- Any repairs as required to keep the laptop in a "ready to learn" state.
- Regular software updates as required by the operating system and antivirus software.

Data security and backups

Students must understand the importance of backing up data securely. Should a hardware or software fault develop, assignment work that has taken a considerable time to prepare may be lost.

The student is responsible for the backup of their personal data. It is recommended that students utilise the education department provided storage space on OneDrive for backing up schoolwork.

Students should also be aware that, if they need to have their computer repaired by an external provider that the contents of the device may be deleted and the storage media reformatted, thus the importance of backup.

Students should ensure that their computer software and antivirus is always kept up to date.

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 Responsible Behaviour Plan, a copy of which is available on the school's website, also supports students by providing school related expectations, guidelines and consequences.

Health and Safety Considerations

Students are encouraged to use their devices in a physically safe manner. This includes:

- Maintaining good posture while using laptops.
- Taking regular breaks to reduce screen time fatigue.
- Using devices in well-lit environments to prevent eye strain.

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 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: Information for parents and carers.

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 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 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.

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 (please consult Technical support table below)
- some school-supplied software e.g. Microsoft Office 365
- printing facilities
- school representative signing of BYOx Charter Agreement.

Student

- participation in BYOx program induction
- acknowledgement that the core purpose of the 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	✗	✓ (Only curriculum related software)
Device vendor		✓ (see specifics of warranty on purchase)	

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

- Use BYO 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, 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 device.
- Use device for private use before or after school.
- Seek teacher's approval where they wish to use a 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 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 Responsible Behaviour Plan.
- The school will educate students on cyber bullying, safe internet and email practices and health and safety regarding the physical use of electronic devices. Students have a responsibility to incorporate these safe practices in their daily behaviour at school.

The school's BYOx program supports personally-owned laptop devices in terms of access to:

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

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.

Device registration and onboarding overview

To ensure secure and reliable access to the school's digital learning environment, all student devices must be registered and onboarded to the school network using the approved process. The following outlines these procedures:

Step 1: Pre-Registration Preparation

- Ensure the device meets the school's minimum specifications.
- Install required software including:
    - Antivirus/security suite (e.g., Microsoft Defender, Norton, McAfee)
    - Microsoft 365 (free for state school students)
    - Internet browsers (Edge, Chrome, Firefox)
- Ensure the student has:
    - A local administrator account on the device
    - Their school-issued Microsoft 365 username and password

Step 2: Onboarding to the School Network

- Devices must be connected to the school's secure wireless network via Education Queensland's BYOx Link (Microsoft Intune) platform.
- Platform specific instructions for onboarding are available on the school website and student SharePoint.
- Students are encouraged to complete onboarding at home before the first day of school.

Step 3: Support and Troubleshooting

- Technical support will be available via the school IT technician or the library before school and during breaks.

Step 4: Daily Use and Monitoring

- Once registered, devices should automatically connect to the school network (EQNet) each day.
- Students must verify connection at the start of each school day.
- Devices must not use personal hotspots or VPNs while on school grounds.

Important Notes

- Devices with incompatible operating systems (e.g., ChromeOS, AndroidOS, Linux, ARM-based Windows) cannot be onboarded.
- Security software that blocks network access (e.g., Microsoft Family, Qustodio) must be configured appropriately to allow for access to the school network.
- Devices can only be onboarded to one school or workplace at a time. If the device has been previously connected to another system outside of Education Queensland, you will need to disconnect the device from the previous location prior to onboarding.
- All internet activity on the school network is monitored and subject to audit.

Frequently Asked Questions

Do I need to bring my laptop to school every day?
Yes. Laptops are essential tools in each year level and every classroom.

How do I protect my device?
It is the student's responsibility to always have their device with them. Protective equipment such as bags or cases should be used to keep these devices safe while at school, and travelling to and from school. It is the responsibility of the student to look after the device while at school and kept securely in bags.

Do I need to back up?
Yes. It is the student's responsibility to back up their files. The school assessment policy clearly states that loss of data due to technology problems is not an acceptable reason for assessment extensions.

We already have a device at home; can I use it at school?
Yes, as long as the device is a laptop and it meets the minimum hardware requirements to connect to the network as outlined in our minimum device specifications fact sheet found on our website.

Will every device work inside the Education Queensland network?
No. Some devices that do not meet our specifications have been found to not connect to the EQ network. These devices may have difficulty with the security filters used by Education Queensland or just fail to see/connect to the network architecture. Ensure that the device you wish to connect is a laptop and that it meets the requirements of the minimum specification guide. Please check with the school if you have any trouble with specifications.

Will the school assist me with network connection settings at school?
Connection from home before school commences is the preferred method, instructions to connect to the network are available on our website. Assistance is available at the IT Help Desk before school and during each break to support students in joining the network. If a device cannot be connected for technical reasons, students will be advised of actions to take to facilitate the connection if the device meets the minimum specifications.

Will the school protect the device from virus attacks?
Virus protection remains the responsibility of the owner. The school has an enterprise model to protect students and our network, however local intrusion to a machine is still possible outside of school and when using USB devices. Students are not able to share viruses across the network, however they should make every effort to make sure there are no viruses present before connecting to the network.

Do I need 3G/4G/5G internet access on the device?
Private internet services are not to be used at school. The school has an effective wireless network available and it is both the education department and the school's policy that whilst at school the school network must be used. This is to help protect students from unsafe and unfiltered/unmonitored internet access. This is a policy that students must adhere to.

Does the school provide software for my BYO device?
The Microsoft Office Suite is available free of charge for five student downloads at home. Specialist software required for some subjects will be provided to students enrolled in those courses. If there are costs involved this will be clearly communicated and included in their course fees.

Can I take my BYO device to IT for repair?
The IT Department cannot perform any software or hardware repairs on a privately owned device. You must seek external IT assistance for these issues.

Will the school assist me with home internet connection settings and issues?
No. Your home internet provider or personal computer technician can assist you with these enquiries.

Will the teacher be able to provide technical support in class?
The teachers are not required to provide IT assistance past the point of explaining where to access the resources they will be using in their class. The IT Department is open before school and during break times to assist students in connecting to the network and to help with curriculum software.

Acceptance of Policies

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

- I have read and understood the BYOx Charter and the school Responsible Behaviour Plan.
- I agree to abide by the guidelines outlined by both documents.
- I am aware that non-compliance or irresponsible behaviour, as per the intent of the BYOx Charter and the Responsible Behaviour Plan, will result in consequences relative to the behaviour.

Please complete and sign this form and return it to Admin

Student's name: _____ **Year:** _____

(Please print)

Student's signature: _____ **Date:** / /

Parent/Caregiver's name: _____

(Please print)

Parent/Caregiver's signature: _____ **Date:** / /