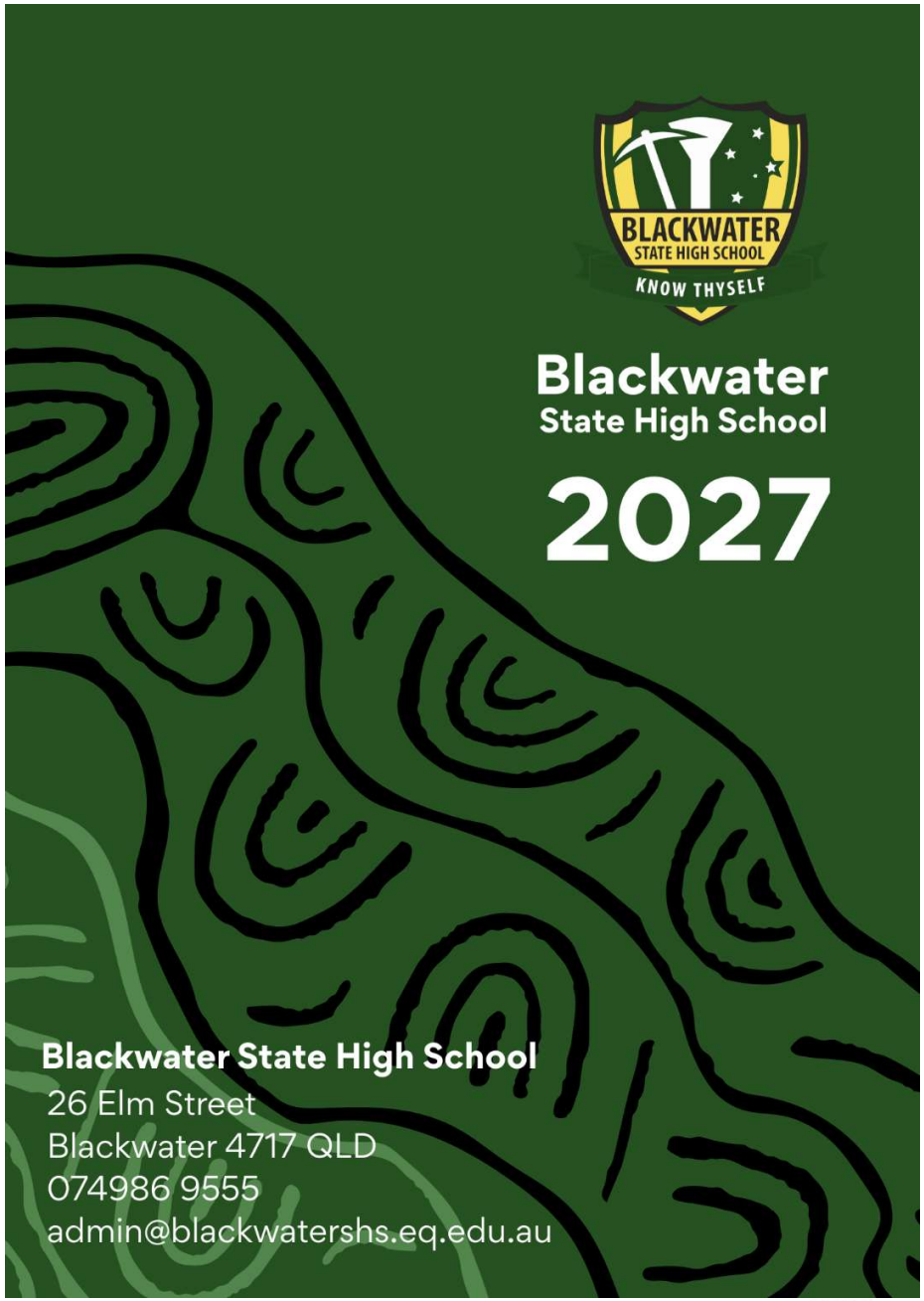
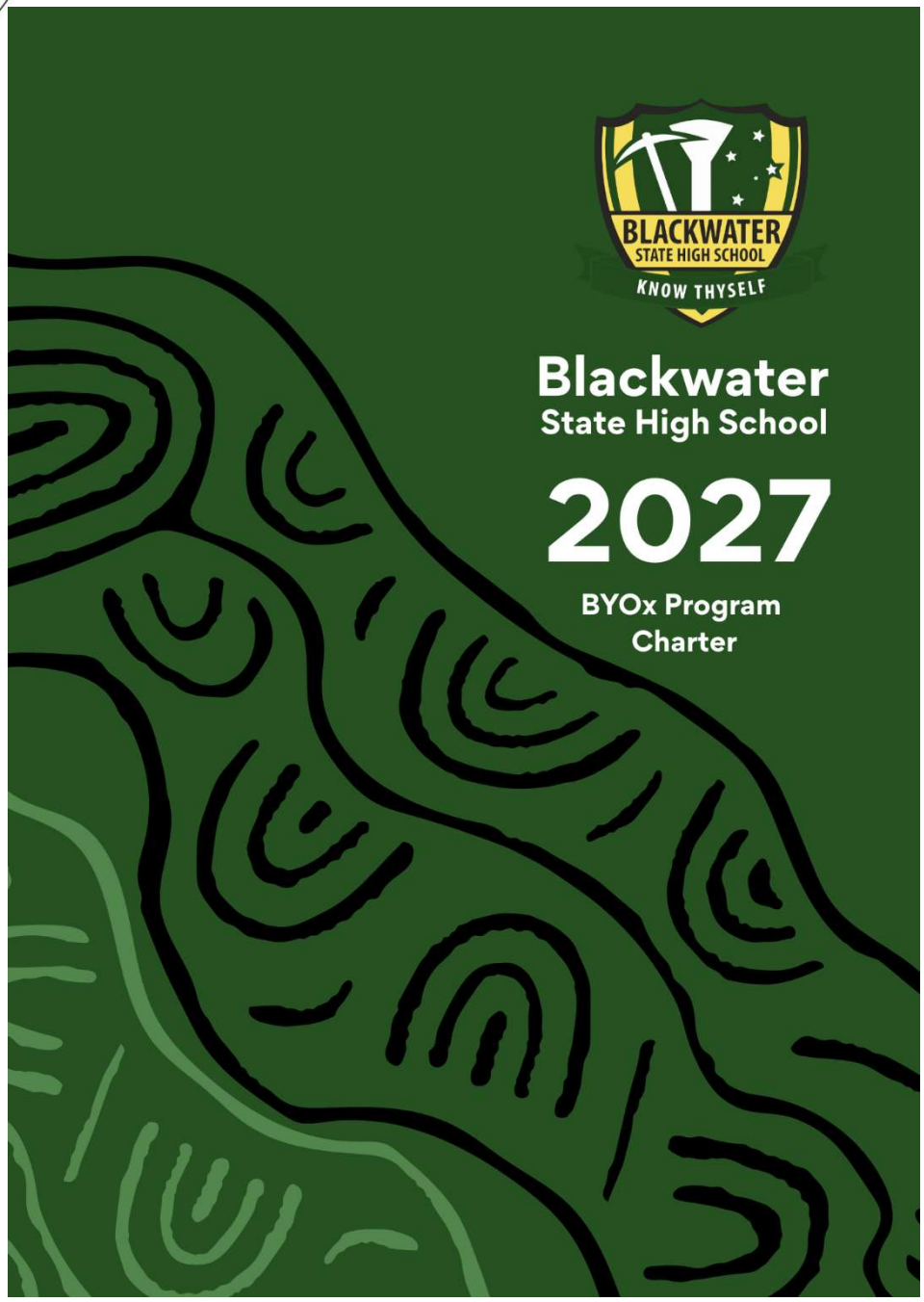

BLACKWATER
STATE HIGH SCHOOL
KNOW THYSELF
Blackwater
State High School
2027
Blackwater State High School
26 Elm Street
Blackwater 4717 QLD
074986 9555
admin@blackwatershs.eq.edu.au


BLACKWATER
STATE HIGH SCHOOL
KNOW THYSELF
Blackwater
State High School
2027
BYOx Program
Charter

Purpose

This charter outlines the expectations, responsibilities and support arrangements for students participating in the Blackwater State High School BYOx program. It is intended to help students and families understand device requirements, safe use expectations and available support.

1. AN OVERVIEW OF THE BYOX PROGRAM 4

2. OPTIONS FOR GETTING A DEVICE 5

3. GETTING THE RIGHT BYOX DEVICE 6

MINIMUM DEVICE REQUIREMENTS 6
RECOMMENDED ACCESSORIES AND PROTECTION 7
UNSUPPORTED DEVICES 7

4. OVERVIEW OF RESPONSIBILITIES 8

RESPONSIBILITIES OF THE SCHOOL 8
RESPONSIBILITIES OF THE STUDENT 8
RESPONSIBILITIES OF THE PARENT/CAREGIVER 9
DEVICE TECHNICAL ISSUES AND SUPPORT 9

5. ENROLLING YOUR BYOX DEVICE 10

INTRODUCTION 10
BEFORE YOU BEGIN 10

6. CARING FOR YOUR BYOX DEVICE 14

DEVICE LABELLING 14
TRANSPORTING AND STORING YOUR DEVICE 14
CHARGING YOUR DEVICE 14
CLEANING AND PREVENTING DAMAGE 15
SOFTWARE AND APP INSTALLATION 15
KEEPING YOUR DEVICE UP TO DATE 15
ANTIVIRUS AND SECURITY SOFTWARE 15
DAMAGE, REPAIRS AND RESPONSIBILITY 16
DATA BACKUPS 16

intentional blank page

Helping protect your student online

Parents/caregivers can help students recognise online risks and respond safely.

It is helpful to:

- explain that not everything online is safe, accurate or appropriate
- talk about the types of content that may be upsetting, inappropriate or unsafe
- help students recognise warning signs such as scams, suspicious links, requests for personal information, or harmful and offensive content
- remind students never to share personal details online unless they are certain it is safe and appropriate
- encourage students to speak to a trusted adult if they see something online that worries them or makes them uncomfortable

Families may also choose to use home internet filtering or safety tools to help manage access across multiple devices in the home.

Reporting concerns

If a parent/caregiver becomes aware of a serious online safety concern affecting a student, they are encouraged to contact the school for support where appropriate.

Further information

Parents/caregivers are encouraged to use trusted and up-to-date sources of information about online safety, cyberbullying, privacy and social media.

Further information can be found at:

- Queensland Department of Education: https://education.qld.gov.au/
- eSafety Commissioner: https://www.esafety.gov.au/

7. RESPONSIBLE USE OF ICT AND INTERNET SERVICES 18

USE OF THE DEPARTMENT OF EDUCATION NETWORK AND INTERNET SERVICES 18
MANAGED INTERNET SERVICES AND INTERNET FILTERING 19
MONITORING, AUDIT AND REPORTING 19
INTELLECTUAL PROPERTY AND COPYRIGHT 20
SOFTWARE 20
SCHOOL EMAIL AND ONLINE COMMUNICATION 20
DIGITAL CITIZENSHIP 21
MISUSE AND BREACHES OF ACCEPTABLE USE 21

8. KEEPING YOURSELF SAFE ONLINE 22

CYBER SAFETY 22
UNSAFE ONLINE CONTENT 22
WEB SAFETY 22
SOCIAL MEDIA SAFETY 23
ONLINE MESSAGING SAFETY 23
CYBERBULLYING AND RESPECTFUL ONLINE BEHAVIOUR 23
PRIVACY AND CONFIDENTIALITY 24
SCAMS AND PHISHING 24
PASSWORDS 25
DEVICE SECURITY AND UPDATES 26
GENERATIVE AI 26

..... 17

9. SUPPORTING SAFE ONLINE USE AT HOME 28

SETTING BOUNDARIES 28
MONITORING AND STAYING INVOLVED 28
SHARE THE EXPERIENCE 29
USE PARENTAL CONTROLS WHERE APPROPRIATE 29
HELPING PROTECT YOUR STUDENT ONLINE 30
REPORTING CONCERNS 30
FURTHER INFORMATION 30

1. An overview of the BYOx program

Blackwater State High School continues to support the BYOx program to help make sure students are prepared for learning in a digital environment. The program applies to all students in Years 9 to 12.

This charter outlines how BYOx works and the expectations for students participating in the program. Participation in the BYOx program is subject to the expectations and responsibilities outlined in this charter.

The term BYOx is used by the Department of Education to describe the teaching and learning environment used in Queensland state schools where students use personally owned mobile devices. The 'x' in BYOx represents more than the device itself and may also include software, applications, accessories, connectivity and carriage services.

BYOx devices are intended to support learning at school and at home. Students are expected to bring their device to school each day charged and ready for use in classroom learning.

The school supports the BYOx model because it:

- supports learning across school, home and other settings
- helps students participate in a modern digital learning environment
- builds everyday digital literacy skills
- supports students to become safe and responsible digital citizens
- enhances teaching and learning through the effective use of technology
- helps prepare students for further study, training and future employment

Share the experience

Taking an interest in how students use technology can help build confidence, trust and safe habits.

- Parents/caregivers may wish to:
- ask their student to show how they use the device for school work
- ask their student to explain the apps, websites or tools they use
- explore positive, educational and interesting online content together
- encourage their student to think critically about online information by asking questions such as:
    - Who created this content?
    - Is this information factual, or is it opinion?
    - Is this website trying to inform, influence or sell something?
- spend time becoming familiar with the device and software so they can better support their student

Use parental controls where appropriate

Parental controls are available on most devices, apps, browsers and home internet services. These tools can help families manage access to content, set time limits and support safer online use.

Parents/caregivers may wish to:

- review and apply parental controls that are appropriate for the student's age and needs
- password protect parental control settings so they cannot be changed without permission
- consider applying parental controls or filtering settings on the home router or network as well as on individual devices

9. Supporting safe online use at home

Parents/caregivers play an important role in helping students use digital devices and the internet safely, responsibly and effectively at home. The following advice may be used to help families support safe online behaviour, healthy routines and positive device use outside school.

Setting boundaries

Students do not need to use their device all the time at home. Setting clear expectations can help support healthy routines, balanced screen time and safe device use.

Parents/caregivers are encouraged to decide:

- where in the home the device can be used
- where the device should be stored when it is not in use
- when the device can be used for school work and when it should be put away
- whether devices should be used in bedrooms or only in shared family spaces
- how device use will be balanced with sleep, physical activity, family time and other offline activities

Monitoring and staying involved

Talking openly about online activity can help students make safer choices and feel more comfortable asking for help if something goes wrong.

Parents/caregivers are encouraged to:

- talk regularly with their student about how they use the internet and digital devices
- encourage device use in a shared family area where appropriate
- monitor the amount of time spent online and the types of websites, apps and services being used
- remember that mobile phones and other digital devices can also provide internet access and may need similar supervision

2. Options for getting a device

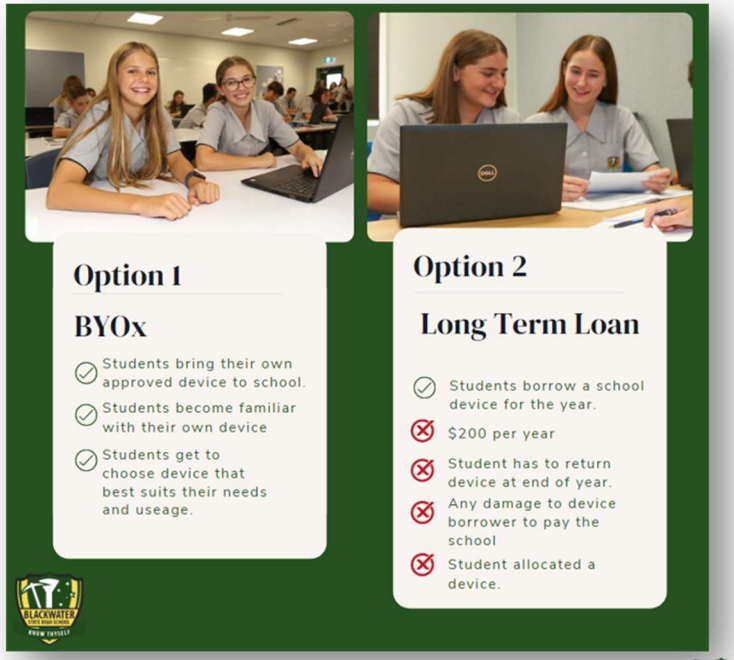
Students in Years 9 to 12 are required to have access to a device for use in class. The school understands that some families may not have an appropriate device available for their student and have made support options available. Please contact the school to discuss what support options are available.

The school offers a long-term loan device option for families through an application process. Loan application paperwork is available from the front office. The cost of a full-year loan is $200 per year, with adjustments available if a device is borrowed part-way through the year or returned before the end of the year.

Loan devices provided by the school meet the school's BYOx requirements and may be taken home each day for school work, assignments and study. A charger is included with each loan device.

Families are expected to take reasonable care of any loan device provided by the school. If a loan device is damaged, lost or not returned, families may be required to pay for repairs or replacement, subject to part pricing and availability.

The school recognises the cost-of-living pressures facing families and has worked to keep both school fees and the BYOx loan fee as low as possible.



3. Getting the right BYOx device

Choosing the right BYOx device is important to make sure students can fully participate in learning and access the school's network, software and online services. Not all devices are supported by the school's BYOx program, so families should check the minimum device requirements carefully before purchasing a device.

The minimum device requirements below are designed to ensure that all students have a device that is compatible with classroom activities and school systems. Features such as touch capabilities, screen size, keyboard layout, weight and finish are largely a matter of personal preference, and families are encouraged to discuss these options with their student when selecting a device.

All BYOx devices must meet the minimum requirements. Devices that do not meet these requirements are considered unsupported. Older devices, particularly those that are five or more years old, may be less reliable and may not meet current performance or security requirements. Families should consider the age and condition of a device when deciding whether it is suitable for school use.

Minimum device requirements

All BYOx devices are required to meet the following minimum specifications:

- Processor: Intel Core 3, AMD Ryzen 3, or better
- Memory: 16 GB or more
- Storage: 256 GB or more
- Operating system: current version of Windows 11
- Battery life: at least five hours of normal use

intentional blank page

Device security and updates

Keeping your device secure is an important part of cyber safety. Students should keep their device operating system, apps, browser and antivirus software up to date to help protect against potential security risks, malware and other harmful software.

Students should use a secure screen lock, only install apps or software from trusted sources, and avoid downloading files or programs from unknown websites or links. Devices should be checked regularly for security issues and suspicious activity.

If a device is believed to be infected with a virus or malware, or is behaving unusually, it should be reported to a parent, caregiver or teacher as soon as possible.

Generative AI

Generative AI tools can be useful for learning, research, planning and creativity when used appropriately. However, they must be used carefully and responsibly. Information produced by generative AI may be incorrect, biased, incomplete or unsuitable for school work unless it has been checked carefully.

Students should only use generative AI tools in ways that are permitted by their teacher and the school. Work submitted for assessment must always meet the school's academic integrity requirements. Students must not use generative AI to cheat, complete work dishonestly, or present AI-generated content as their own where this is not allowed.

Students should never enter personal, confidential or sensitive information into generative AI tools. This includes their own personal information, the personal information of others, school records, assessment materials or any other private or restricted information.

If a student is unsure whether a generative AI tool can be used for a task, they should ask their teacher before using it.

Recommended accessories and protection

Families are encouraged to consider practical items that support daily use at school. A protective case or sleeve is strongly recommended to help reduce the risk of damage during transport and storage. Useful accessories such as wired headphones and a mouse may also be brought to school to support learning and improve usability.

Unsupported devices

Devices that do not meet the minimum device specifications are not supported by the school's BYOx program. These devices may be unable to connect to the school network, may not be compatible with required educational software, and are not eligible for school-based technical support.

Devices that are not running a current version of Windows 11 are considered unsupported. This is to maintain network compatibility, security requirements and a consistent teaching and learning environment for all students and staff.

Unsupported devices include:

- Chromebooks
- Apple devices, including iPads and MacBooks
- devices that do not meet the minimum hardware requirements listed previously

4. Overview of responsibilities

The BYOx program is a shared responsibility between the school, students and parents/caregivers. Each party plays an important role in supporting safe, effective and reliable use of BYOx devices for learning.

Responsibilities of the school

The school is responsible for:

- Maintaining the school ICT network and related services
- Providing access to school-supported internet services and internet filtering while connected to the Department of Education network
- Maintaining school-provided digital storage, network services and other school-supported online systems
- Providing access to approved school-supplied software where applicable
- Providing access to printing services in accordance with school processes, availability and any applicable limits
- Supporting students and families with information about the school's BYOx requirements and expectations
- Managing the school's loan device process, subject to availability

Responsibilities of the student

Students are responsible for:

- participating in the BYOx program in accordance with this charter
- bringing their BYOx device to school charged, ready for use and suitable for learning
- using their BYOx device safely, responsibly and respectfully
- using the school network, internet services and online communication tools appropriately
- caring for and maintaining their personal device and accessories
- respecting the property, privacy and digital safety of other students and staff
- regularly backing up important files and school work
- protecting their personal information, passwords and account access
- taking appropriate steps to maintain cyber security and online safety

Passwords

Passwords help protect access to your digital accounts and personal information. Using strong and secure passwords can reduce the risk of unauthorised access, account breaches, lockout and identity theft. When creating a password, use a different password for each account, make sure it is not easy to guess, and use at least eight characters.

The Department of Education applies password requirements to student network accounts, and these passwords must be changed periodically. The requirements below are provided to help students remember the rules for their school account and can also be used as a guide when creating passwords for other accounts.

Student account password rules:

- New passwords cannot have been used during the previous 13 password changes.
- Passwords must be at least eight characters long.
- Passwords must not contain all or part of the user's account name.
- Passwords must contain characters from three of the following four categories:
    - uppercase letters (A to Z)
    - lowercase letters (a to z)
    - numbers (0 to 9)
    - non-alphabetic characters, such as $, # or %

Never share your password or account login details with anyone or use the password or account of someone else If anyone asks for your password or account details, report it to a parent, caregiver or teacher.

Students must never send, post or share content that is inappropriate, offensive, abusive, threatening, bullying, harassing, discriminatory, sexually explicit, sexually suggestive, false or defamatory. If a student experiences or witnesses cyberbullying, they should report it to a parent, caregiver or teacher immediately.

Privacy and confidentiality

Protecting your privacy and the confidentiality of others is an important part of staying safe online. Students should never share personal information online, especially with people they do not know. This includes names, addresses, photographs, phone numbers, email addresses, financial details and other private information.

Students must not publish or share any of the above details of another student or staff member without that person's permission. Privacy and confidentiality should always be respected when using digital devices, online services and school systems.

If a student is asked to share personal information, use someone else's account, or access information they should not have access to, they should report it to a parent, caregiver or teacher.

Scams and phishing

Scams and phishing attempts are common online and are often designed to trick people into sharing personal information, passwords or financial details. These attempts may appear in emails, messages, pop-up windows, social media posts or websites, and may look genuine at first glance.

Students should be cautious of unexpected messages, urgent requests, offers that seem too good to be true, or links and attachments from unknown sources. Never provide personal information, account details or passwords in response to an unsolicited message or website request.

If a student receives a suspicious message, link or request, they should not respond, click on any links or open any attachments. It should be reported to a parent, caregiver or teacher.

- reporting damage, lost equipment, security concerns or technical issues promptly to the school and parent/caregiver
- complying with this charter, the school's Student Code of Conduct, and other relevant school expectations

Responsibilities of the parent/caregiver

Parents/caregivers are responsible for:

- supporting and encouraging their student's participation in the BYOx program
- helping ensure the student has access to a suitable and supported device
- supporting the care, maintenance and safe transport of the student's BYOx device
- helping ensure the device is protected by an appropriate bag, sleeve or carry case
- monitoring and supervising internet access outside the Department of Education network where appropriate
- supporting the student to use the device safely, responsibly and in accordance with school expectations
- assisting with device maintenance, repairs and software installation where required
- meeting costs associated with repair, replacement, accessories or insurance for personally owned devices

Device technical issues and support

Students and families are responsible for the operation, care, maintenance and repair of personally owned BYOx devices. The school and the Department of Education are not responsible for damage, loss or theft of personal devices brought to school.

School ICT technicians can assist with issues relating to school network access, connectivity to school systems and other school-provided services where appropriate. Technical issues relating to the device itself, its hardware, the operating system, or software not provided or required by the school must be resolved by the student, parent/caregiver, device supplier or repair provider.

Families are encouraged to make sure that devices are covered by warranty and, where possible, accidental damage protection or insurance.

5. Enrolling your BYOx device

Introduction

Before a personal BYOx device can access the school Wi-Fi, email, learning applications and other school online services, the student's school account must be added to the device.

These instructions explain how to add a school account to a personal Windows 11 device through Settings > Accounts > Access work or school. This process usually takes around 5 minutes to complete.

Before you begin

Before starting, please make sure:

- the device is running the current version of Windows 11
- the device is connected to the internet
- the device is charged or connected to power
- the student's school email address and password are available

If you do not have the student's school login details, please contact the school before continuing.

Only supported Windows 11 devices can be connected to the school's BYOx program.

Some screens may look slightly different depending on the version of Windows installed, device settings, personalisation configurations, or any updates made since these instructions were prepared.

This setup usually only needs to be completed once for each device, unless the school account is removed or the device is reset.

If the setup process does not complete successfully, close the settings window, restart the device and try again. If you continue to experience difficulties adding the school account or accessing school services afterwards, please contact the school for assistance.

Important: Device enrolment should be completed at home or in another location with a reliable internet connection before the device is brought to school for use.

Social media safety

Social media can be a positive way to communicate, share ideas and stay connected. However, it can also expose students to unsafe content, scams, cyberbullying, privacy risks and contact from strangers.

Students should think carefully before posting, sharing images, commenting or interacting online. Information shared on social media can be difficult to remove and may be seen by a wider audience than intended. Students should use privacy settings, avoid sharing personal information, and only connect with people they know and trust.

If a student sees or experiences anything unsafe, inappropriate or upsetting on social media, they should report it to a parent, caregiver or teacher.

Online messaging safety

There are many ways to communicate online, including messaging, email, chat services and file sharing. These tools can be useful and positive, but they can also be used for harmful or malicious purposes. To help keep yourself safe, only communicate with people you know and do not accept message requests from strangers or unknown accounts.

If you receive a message from someone you do not know, or a message that contains suspicious, harmful or inappropriate content, report it immediately to a parent, caregiver or teacher. This includes unsolicited messages, requests for personal information, offers of gifts, requests to speak by phone, or any attempt to arrange an in-person meeting. Never click on links, follow instructions or open files unless you can confirm they come from a legitimate and trusted source.

Parents, caregivers and students are encouraged to read the department's Cybersafety and Cyberbullying Guide for Parents and Caregivers. For a copy, please contact the school or refer to the Department of Education website.

Cyberbullying and respectful online behaviour

Students are expected to behave respectfully online at all times. Online communication should be used in a way that is safe, responsible and considerate of others. Behaviour that is bullying, threatening, abusive, harassing, discriminatory or intended to harm another person is not acceptable.

Cyberbullying can occur through messages, social media, online games, group chats, email or other digital platforms. It may include repeated hurtful messages, sharing embarrassing images or information, excluding others online, impersonating someone, or posting harmful comments.

8. Keeping yourself safe online

Cyber safety

Making sure you stay safe online is important. With the growing amount of unsafe content, scams and malicious actors online, cyber safety should be a priority whenever you access the internet. This section includes important topics, advice and recommendations to help keep you, your personal information and your device safe, while supporting positive, responsible and respectful online experiences.

Unsafe online content

The internet contains a large amount of content, and much of it can be positive, useful and helpful. However, it can also contain unsafe or inappropriate content. This content may appear on websites, social media, online games, messaging platforms and advertisements, and may be shared by people seeking to cause harm, spread harmful ideas or commit cyber crime.

Unsafe or inappropriate content may put you, your personal information or your device at risk, or may include material that is illegal or not suitable for minors. This can include hateful or disturbing content, malicious software, unsafe downloads, pirated content, scams, unlawful sales, and contact from unknown or suspicious individuals.

If you find or are sent unsafe or inappropriate content, do not engage with it. Report it to a parent, caregiver or teacher. If you are unsure about something you see online, speak to a parent, caregiver or teacher to help you make a safe and informed choice.

Web safety

The internet hosts a large number of websites. Many are helpful, educational and enjoyable to use, but some should be avoided. Certain websites contain malicious, dangerous or inappropriate content and may put you, your personal information or your device at risk.

Turning on safe search settings in your browser can help reduce the chance of unsafe websites appearing in search results. To further protect yourself, avoid visiting websites you do not recognise or websites with unusual or suspicious web addresses. Avoid clicking on links unless you are confident they are genuine.

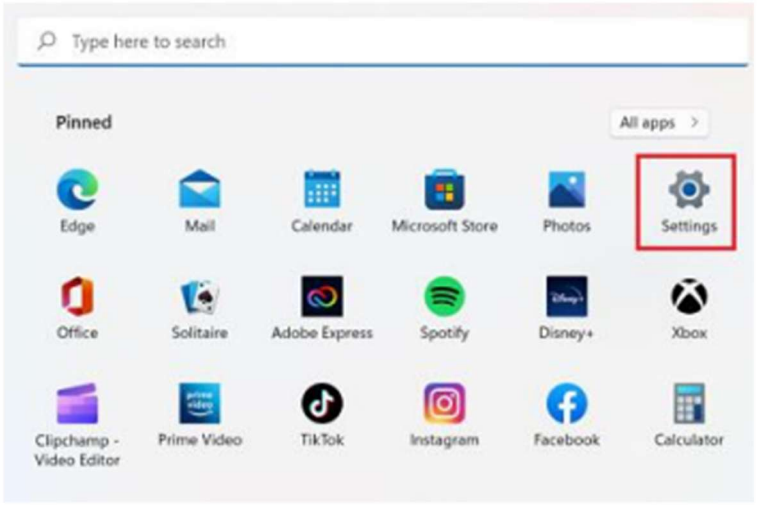
Never enter personal, financial or medical information into a website unless you can confirm that it is legitimate and safe. If you find or are sent a suspicious or harmful website or link, report it to a parent, caregiver or teacher.

Step 1 – Install Intune

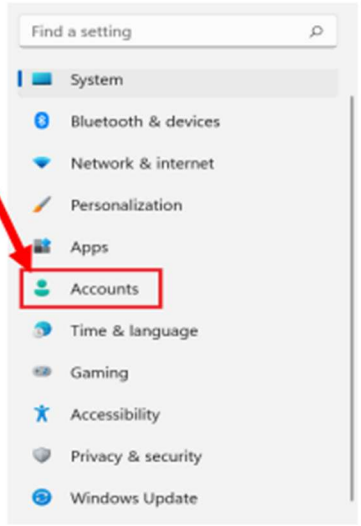
a. Connect to the internet and select the Windows icon at the bottom of your screen.



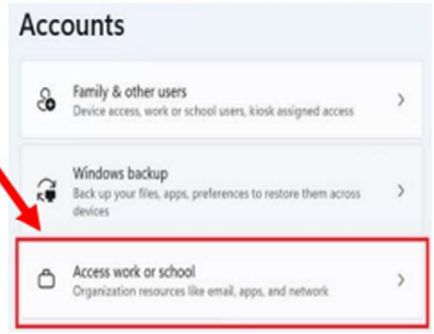
b. Select the **Settings** icon.



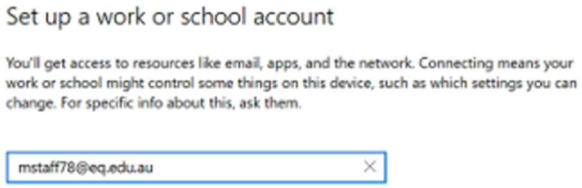
c. Select **Accounts**.



d. Select **Access work or school**. If your account is already listed, select it and then select **Disconnect**. Then select **Connect**.



e. Enter your school @eq.edu.au email address and select **Next**.



Digital citizenship

Students are expected to be safe, responsible and respectful digital citizens. This includes thinking carefully about what they create, share, post and communicate online, and understanding that online actions can affect their reputation and the wellbeing of others.

Students should be mindful that online content may be searchable, copied, shared and remain accessible into the future. Behaviour in digital spaces should reflect the same standards of safe and respectful behaviour expected at school and in the broader community.

Parents/caregivers are encouraged to support students in understanding these responsibilities and in developing positive online habits.

Misuse and breaches of acceptable use

Students are responsible for their actions when using ICT and internet services. Students may also be held responsible if they knowingly allow another person to use their account, password or device in a way that breaches school or departmental expectations.

The school may restrict or remove access to digital devices, the school network, internet, email or other ICT services where necessary to protect the security and integrity of systems or to maintain a safe learning environment.

Misuse of ICT or internet services may result in disciplinary action in accordance with the school's Student Code of Conduct. This may include the withdrawal of access to school-provided ICT services.

Intellectual property and copyright

Students must respect copyright, intellectual property and the work of others when using ICT services. Information, images, audio, video and other material used in school work should be properly acknowledged where required.

Students must not plagiarise the work of others or present another person's work as their own. Students must also obtain appropriate permission before publishing, sharing or reproducing another person's work, image or creative content where permission is required.

Any school-related content posted on the internet must have appropriate approval and comply with copyright requirements and school processes.

Software

The school may require or recommend software applications to support curriculum delivery and learning. Parents/caregivers may be required to assist with installing and maintaining approved software in accordance with school guidance.

Students must not possess, use or distribute unlicensed, unauthorised or pirated software. Software installed on a student device should only be obtained from trusted and legitimate sources, such as the official software provider's website or app store.

When a student leaves the school, transfers or graduates, it is recommended that school-related accounts, software and access arrangements are removed from the device to help prevent future access or account conflicts.

School email and online communication

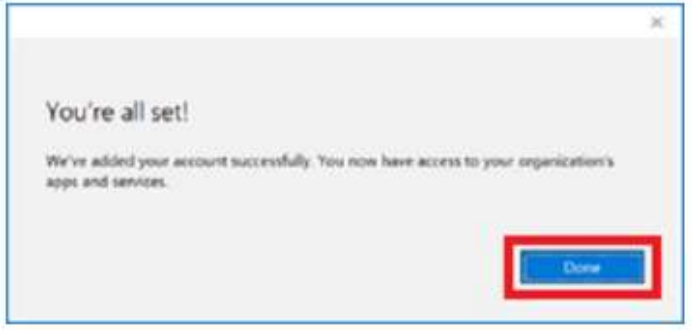
Students must use school email and other school-supported communication tools appropriately and for educational purposes. Messages should be respectful, relevant and suitable for a school environment.

Students must not use school email or online communication services to send spam, hoax messages, chain messages, harmful attachments, offensive content or messages intended to harass, threaten or mislead others.

f. Please enter your username, password, accept the terms and conditions, and **Sign in**.



g. Please select **Done**.



h. Check your account has been added. Your account details will be displayed.



If you need help enrolling your device, please visit the Tech Hub in the resource centre during school hours, where a staff member can assist you.

6. Caring for your BYOx device

Looking after your BYOx device is important to help keep it safe, reliable and ready for learning. The information below provides practical advice to help you take care of your device, maintain its performance and reduce the risk of damage.

Device labelling

Students are encouraged to clearly label their device, charger and any accessories with their name. Labelling helps identify devices and equipment if they are misplaced, left behind or mixed up with similar items belonging to other students.

Labels should be placed in a secure and visible location without covering vents, ports, cameras or other important parts of the device.

Transporting and storing your device

Devices should be carried in a protective laptop case or sleeve when travelling to and from school. This helps reduce the risk of damage from drops, pressure, dust and spills. A dedicated laptop compartment or protective bag is recommended where possible.

When not in use, devices should be stored safely and securely. Students should not leave their device unattended, loosely packed in a bag, or placed where it may be damaged by heavy items, food containers or drink bottles. Devices should also be kept away from excessive heat, direct sunlight and moisture.

Before placing a device in a school bag, students should ensure it is shut down or in a safe sleep state and stored securely.

Charging your device

Students should charge their device before bringing it to school each day so that it is ready for learning. Before charging, the charger, cable and charging port should be checked for damage, dirt or debris.

Devices should only be charged using the correct charger and compatible accessories recommended by the manufacturer. Damaged, poor-quality or incompatible chargers and cables may cause damage to the device and create a safety risk.

Devices should be charged in a safe, well-ventilated area and should not be covered while charging. Chargers should be disconnected if they are damaged or become unusually hot. Safe charging practices can help reduce the risk of damage and support battery life.

- photograph, record or share images, video or audio of another person without permission and without an educational or authorised purpose
- use ICT services to cheat, plagiarise, complete assessment dishonestly, or support any other form of academic misconduct

Students must only use departmental ICT services for educational purposes and other approved school-related activities.

Managed internet services and internet filtering

Internet access supports a wide range of learning activities. To help protect students and school networks, the Department of Education uses managed internet services and internet filtering across Queensland state schools.

Devices connected to the Department of Education network may be subject to filtering and other security controls designed to reduce access to malicious, inappropriate or unsafe content. These protections help block harmful websites, malware, spyware, scams, identity theft attempts and unauthorised online activity.

No filtering system can remove every risk. If a student accesses or discovers a website, service or content that is unsafe, inappropriate or not blocked as expected, it should be reported to the school as soon as possible.

Families should also be aware that internet access outside the Department of Education network is not filtered in the same way. Parents/caregivers are responsible for monitoring and supervising internet use outside school where appropriate.

Monitoring, audit and reporting

Students should be aware that use of the Department of Education network, internet services and online communication services may be monitored, logged, audited and traced to the user account involved.

Authorised staff within the Department may investigate suspected misuse of school or departmental ICT services in accordance with school processes, Department procedure and legal requirements.

Students must report any suspected security issue, misuse, harmful content, scam, privacy concern or breach of this charter to a teacher or other appropriate staff member as soon as possible.

7. Responsible use of ICT and internet services

Access to the Department of Education network and internet services is provided to support student learning. Students are expected to use these services safely, responsibly and respectfully, in accordance with the school's Student Code of Conduct and the expectations outlined in this charter.

When a student is enrolled in a Queensland state school, parent/caregiver permission is sought to allow access to the department's ICT network and systems, including internet services. These acceptable use conditions apply when using the device and internet services both at school and, where relevant, off school grounds.

Communication using internet and online services must always be appropriate, respectful and lawful. Students must use ICT resources in a way that supports learning and does not place themselves, others, the school or the network at risk. The use of generative AI tools must also comply with school expectations for academic integrity, privacy and responsible use.

Use of the Department of Education network and internet services

While connected to the Department of Education network or using departmental ICT services, students must not:

- create, access, store or share content that is offensive, inappropriate, unlawful or harmful
- attempt to undermine, bypass, hack or interfere with network security, filtering or other protective measures
- disable or interfere with virus protection, spam filtering, internet filtering or other security settings applied by the school or the Department
- use unauthorised programs, applications or services
- intentionally download, install or distribute unauthorised software, files or other content
- intentionally damage or disrupt devices, systems, services, accounts, software, school networks or government networks
- use ICT services for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose
- use another person's account, login details or identity to access services or information
- collect, store or share another person's personal information without permission or lawful authority

Cleaning and preventing damage

Regular cleaning can help keep a device in good condition and prevent the build-up of dust, dirt and grime that may affect its performance. Screens and keyboards should be cleaned carefully using appropriate cleaning methods recommended by the device manufacturer.

Food and drinks should be kept away from the device, as spills can cause serious damage.

Software and app installation

Students should only install software and apps that are safe, appropriate and needed for learning. Software and apps should only be downloaded from trusted and legitimate sources, such as the official app store or the software provider's website.

Students should avoid installing unknown, unapproved or pirated software, as it may contain malware, affect device performance or create security risks. Students should also remove software that is no longer needed, including expired trial software that may interfere with the device's normal operation.

Keeping your device up to date

Devices receive regular operating system and software updates. These updates may include new features, important security patches and updated drivers that help keep the device secure and working properly.

Students should regularly check for updates and install them as soon as practical. On Windows devices, updates can be managed through the Settings app under Windows Update. Automatic updates should be enabled where possible.

Antivirus and security software

Antivirus and security software help protect devices from viruses, malware and other harmful software. Some laptops are sold with a trial version of paid antivirus software. If this software is not renewed, it should be uninstalled so that the built-in Windows Defender Antivirus can operate correctly.

Expired or conflicting antivirus software can cause problems with device performance and security. Students should ensure that antivirus protection is active and up to date at all times.

Damage, repairs and responsibility

Students and parents/caregivers are responsible for the care, maintenance and repair of the student's device. The school and the Department of Education are not responsible for damage, loss or theft of personal devices brought to school.

Families are encouraged to ensure the device is covered by warranty and, where possible, accidental damage protection or insurance. If a device is damaged or requires repair, students should follow the manufacturer's advice and seek support from the supplier or repair provider.

Data backups

Backing up your data and files is important to help prevent the loss of school work and other important information. Students are encouraged to regularly save and back up their files using reliable storage options. We recommend using the cloud-based storage service OneDrive, which is available to all students. Students may also use the school network storage, or an external storage device such as a USB or external hard drive.

When using local device storage or external storage, students should keep more than one copy of important files and store copies in separate locations where possible. This helps protect against data loss if a device is damaged, lost, stolen or needs to be repaired.

If a device needs to be sent away for repairs, any files stored only on the device may be lost. Students are responsible for backing up their own data and maintaining the integrity of their files. Loss of data, including assessment work, may not be accepted as grounds for an exemption or extension.

intentional blank page