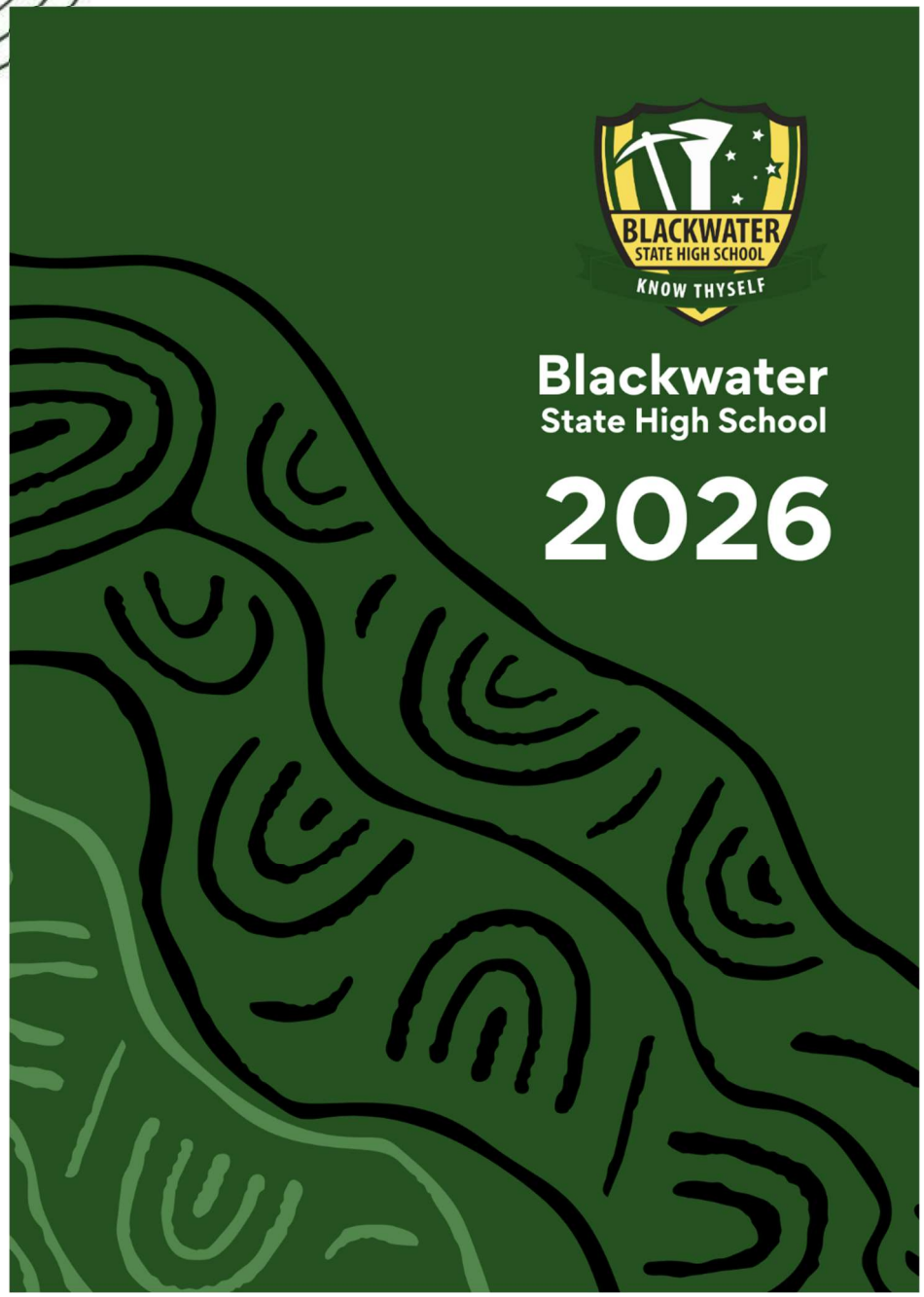
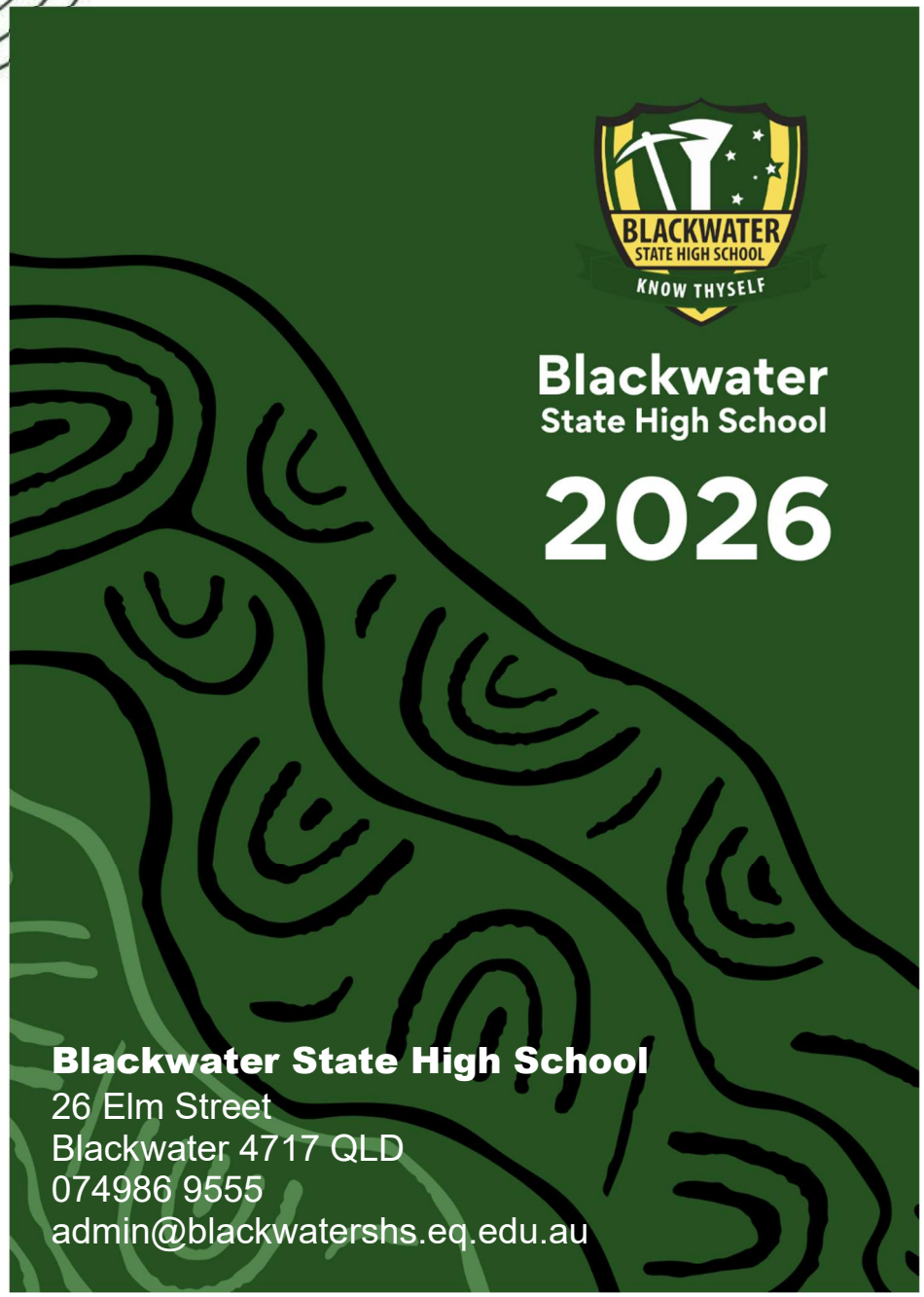

BLACKWATER
STATE HIGH SCHOOL
KNOW THYSELF
Blackwater
State High School
2026

Contents



Further Information

Detailed instructions can be found
http://education.qld.gov.au/learningplace/help/online-safety-support.html

This departmental guide provides important information for parents about cyber safety and cyberbullying. It suggests what parents and caregivers could do if their child is the target of, or is responsible for, inappropriate online behaviour.

http://www.cybersafetyhelp.gov.au/easyguide_Easy_Guide_to_SocialisingOnline

This is a good resource for parents to understand the different social networking sites/apps.

http://www.cybersmart.gov.au/Parents.aspx

http://www.aplatformforgood.org/parents

An Overview of the BYOx Program

Blackwater State High School is continuing on with the success of the pre-existing BYOx program which has been designed to ensure every student is prepared for success in the digital era. The BYOx program is only applicable to students in the Years 9 through to Year 12.

If this is the first year of your student participating in our program, you may be unsure as to how it works alongside the expectations when participating in this program. This charter will be able to explain how the program works.

The BYOx acronym used by the department refers to the teaching and learning environment in Queensland state schools where personally-owned mobile devices are used. The 'x' in BYOx represents more than a personally-owned mobile device; it also includes software, applications, connectivity or carriage service.

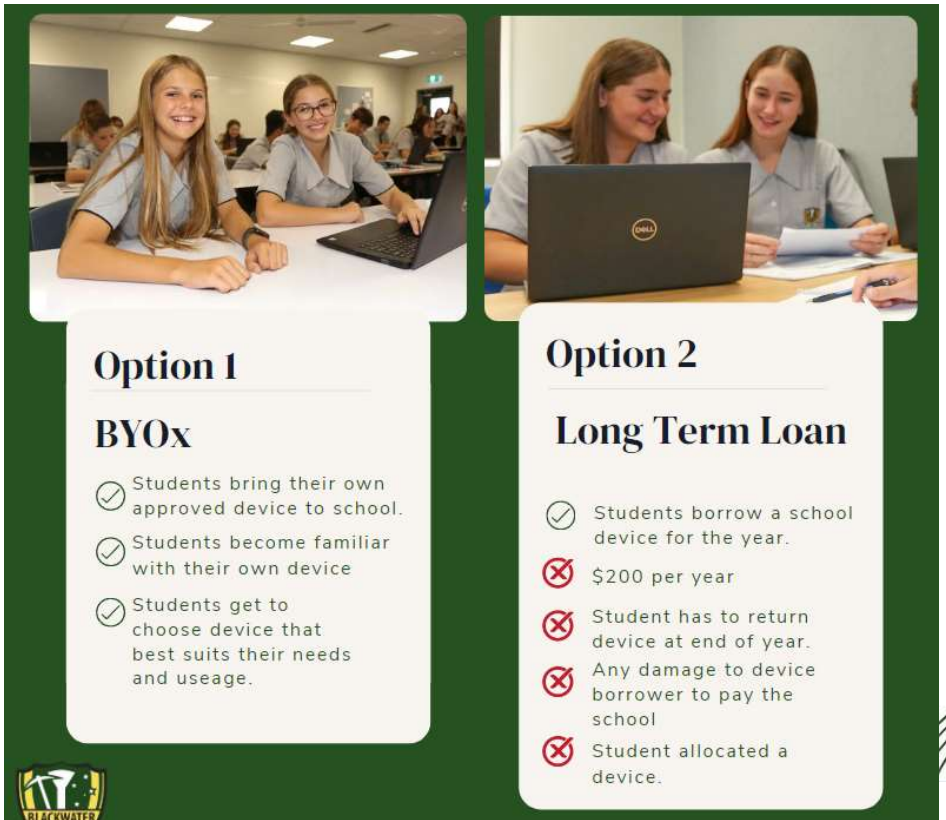
The Department has chosen to support the implementation of a BYOx model because:

- BYOx recognises the demand for seamless movement between school, work, home and play
- Our BYOx program assists students to improve their learning outcomes in a contemporary educational setting
- Assisting students to become responsible digital citizens enhances the teaching learning process
- Achievement of student outcomes as well as the skills and experiences that will prepare them for their future studies and careers.

Device Options

It is a requirement that all students in years 9 – 12 have a device for every class. The school does have provisions should families not have appropriate devices available for a student to bring to school.

The school offers a long-term loan option which is available for families through application. These devices cost $200 per year with this payment being pro-rated should your child purchase a device throughout the year. These loaner devices meet the schools' minimum specifications and students are allowed to take these devices home each day and use them over the holidays. The school has taken into consideration the current cost of living and therefore has strived to keep both school fees and the BYOx loan fee to a minimum.



Parental controls

are available on all devices, please set these as appropriate with your child and password protect the decisions that you have made. The same can be done for your home router or network.

Protect

• Explain to your child that not all information on the internet is good, true or helpful, and that some areas are not intended for children to see.

• Help your child identify unsuitable material by naming some things to look out for, such as sites that contain scary or rude pictures, swearing or angry words.

• Empower your child to use the internet safely by showing your child safe sites and explaining why they are safe. It's also important to educate your child on why it's not safe to give out any personal details online.

• There are many home network filter programs on the market such as OpenDNS, K9 Web Protection. A simple search for 'Home Web Filtering' will give you the current lists; many programs are free. The advantage for parents is that this can be applied to ALL devices in the home.

Supporting Safe IT use at Home

The following advice looks at ways parents can support their student in using the internet effectively, so they can enjoy and learn from the internet safely and securely.

Set Boundaries

Students don't need to use their devices all the time at home. If you are experiencing problems, we recommend that you specify:

- Where in the house the device can be used.
- Where it is to be stored when not in use.

Monitor

- Talk about internet activities openly and freely.
- Have your child use the device in a shared family area where you can monitor how long your child is online as well as the websites your child is visiting.
- Mobile phones and other digital devices have access the internet, so these devices need to be monitored also.

Share the Experience

- Ask your child to demonstrate the way they use their device for school.
- Ask your child to teach you how to use the device.
- Focus on the positive aspects of the internet when you sharing the experience with your child. Spend time looking together at sites that are fun, interesting or educational.
- Encourage your child to question things on the internet, e.g. Who is in charge of this site? Have I found information, or is it just opinion? Is this site trying to influence me or sell me something?
- Have a play with the device and software by yourself to better understand how they work.

Choosing Your BYOx Device

With the endless options for devices, it may seem like a challenging task trying to find the right device for your student.

Understanding the needs of your student is the biggest factor in choosing the right device for you. Students who only use their device for note taking and document editing are going to have lower requirements compared to a student who uses their device for Computer Aided Design or Digital Arts.

Required Specs

- CPU: Intel Core 3 or Better
- Memory/RAM: 8GB or More
- Storage/SSD: 128GB or More
- Operating System: Must use Windows 11

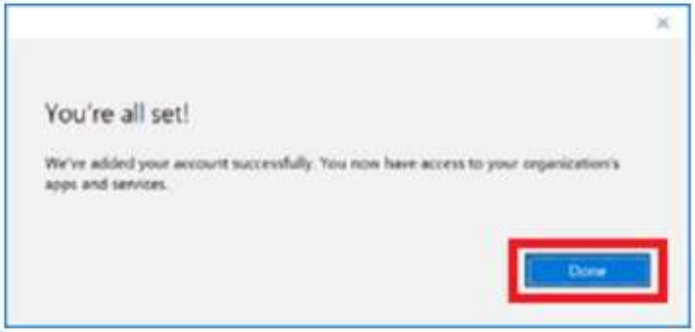
All devices require the following.

- Devices are required to be using the latest version of Windows 11. (Windows 11 version 25H2 at a minimum)
- Chromebook devices are incompatible with the school's BYOx program and cannot be used at school.
- Devices that are 5 Years or older are not recommended due to component degradation and potential incompatibility with the latest windows versions

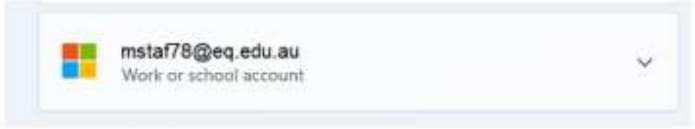
Students are able and encouraged to utilise the web-based versions of the Microsoft 365 package.

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

g. Please select **Done**.

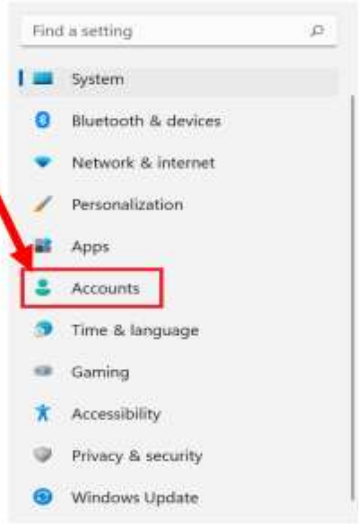


h. Check your account has been added. Your account details will be displayed.

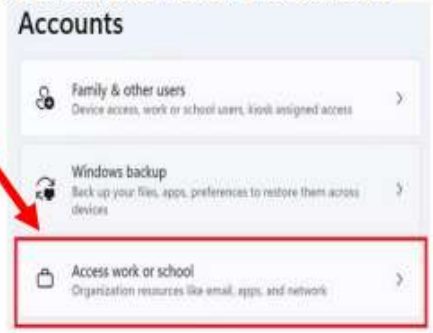


If you require assistance to enrol your device into the school system, please visit the Tech Hub in the library where a staff member will assist you to enrol your device.

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**.

Caring for your BYOx Device

We understand that not everyone is familiar or confident with how to maintain and care for devices. Below are some simple steps to ensure your device is kept at peak performance.

Precautions to be aware of:

- Keep all liquids away from devices
- Keep all food away from devices
- Ensure connectors are properly secured when in use
- Ensure all cables are disconnected before moving the device
- Ensure devices are turned off before storing or placing into a bag
- Devices should only be transported/carried in a dedicated laptop bag or in a dedicated backpack laptop slot/pocket
- Ensure that the battery is charged before coming to school
- Do not leave the device on charge once it is fully charged

Maintenance of Your Device:

- Ensure all drivers are kept up to date
- Ensure that software is kept up to date
- Ensure your operating system is kept up to date
- Ensure that your antivirus in up to date
- Perform regular antivirus scans
- Regularly clean the device's screen and keys
- Ensure that cables and ports are not damaged before use

Please be aware that you and your student are fully responsible for the care and maintenance of your device. The school will not be held liable for any damages that may occur to your device. We recommend that your device is under warranty and has some form of accidental damage cover or insurance. Please consult your manufacture's guides for further maintenance recommendations.

Cyber Safety and Data Protection

Cyber Safety

To ensure your safety online it is important to report anything that seems suspicious or malicious to a parent, caregiver, or teacher. This includes but is not limited to unsolicited emails or messages, suspected virus or malware and other inappropriate content. Students must also seek help if another user requests 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:

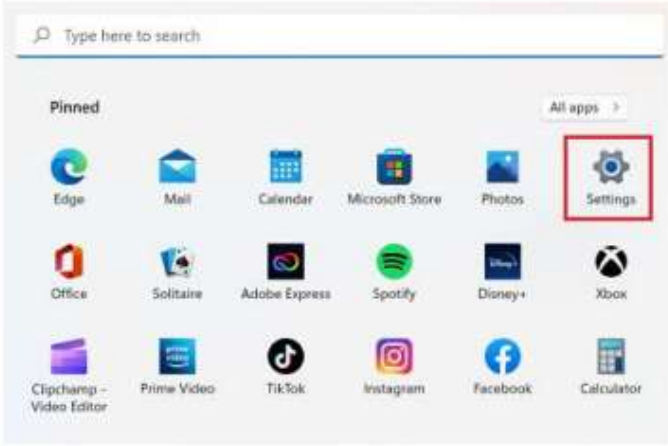
- a message sent to them in confidence
- a computer virus or attachment that can damage the recipients' computer
- chain letters or hoax emails
- spam (such as unsolicited advertising).
- Students must never send, post, or publish:
    - inappropriate or unlawful content, which is offensive, abusive, or discriminatory
    - threats, bullying or harassment of another person
    - sexually explicit or sexually suggestive content or correspondence
    - false or defamatory information about a person or organisation.

Parents, caregivers, and students are encouraged to read the department's Cybersafety and Cyberbullying guide for parents and caregivers for a copy of this please contact the school or refer to Education Queensland's website.

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.



Enrolling Your BYOx Device into Intune

Introduction

Microsoft Intune is a secure mobile management system that allows you to use school Wi-Fi, emails, learning applications and websites on personal devices. These instructions will show you how to enrol a BYO Windows device into Intune and install an application. This process may take up to 15 minutes to complete. Before you start, please have ready the email address and password that has been supplied to you by the school. If you do not have this information, you will not be able to successfully complete the installation. Please contact your school to obtain these details. These instructions are for Windows 11 and above. You may find some of the screens look different to the ones provided here if you have an older version of Windows or there are changes made to Intune. If the installation fails at any time, please re-open the Intune app and try again. Please note: If you have any problems with installing Intune or using it afterwards, please contact your school for assistance.

Passwords

The Queensland Department of Education school networks are secured though the use of unique usernames and passwords. To ensure the integrity of the network and the security of your data it is vital that students do not share their usernames and/or passwords with anyone. Passwords are required to be changed every 180 days.

Passwords are required to meet the following requirements to be suitable to use on the department's network.

- New passwords cannot have been used during the previous 13 password changes.
- The length of the password must be at least eight characters.
- Not to contain all or part of the user's account name.
- The password must contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, $, #, %)

Please note students are responsible for all actions taken on their account including those from users they have knowingly given access to their account.

It is encouraged that student BYOx devices have a local password to ensure only they have access to the device.

Privacy and Confidentiality

Students should never expose personal information via the internet or email especially to unknown entities. 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.

Students are not to use credentials that are not their own to access the Department of Education network. Students are not to access another student or staff member's files, emails network drives or systems. Students are not to or attempt to gain access to content, systems, or files in any illegal or unauthorized manner.

Data Backups

To ensure you never lose any data it is important to keep backups of your data and files. Many solutions can be deployed to achieve this goal, we recommend taking advantage of the cloud-based storage solution, OneDrive that is available to all students. Alternatively, we suggest you use the local network to store your files which can be accessed using the BYOx Mapper application provided from the company portal. The option of using an external hard drive or USB will also be suitable. When utilising local device or external storage, it is important to ensure multiple copies are kept in separate locations to ensure the integrity and safety of your data.

It is important to keep your antivirus up to date and undertake regular scans to prevent malicious virus from corrupting, deleting or stealing your data.

Be aware if your device needs to be sent away for repairs local files on the device may be lost.

Please note the loss of data including assessments will not grant the student any exemption or extension. Students are entirely responsible for the backups and integrity of their data.

Overview of Responsibilities

The Responsibilities of the School

- The maintenance of the school ICT network
- Printing services
- School network drive maintenance
- School network internet filtering
- School supplied software

The Responsibilities of the Student

- Participation in the BYOx Program
- Responsible use of their BYOx device
- Responsible use of the school network and internet services
- Care and maintenance of personal devices
- Respect to other students BYOx devices
- Maintaining current data backups
- Ensuring the integrity of personal information and data
- Taking appropriate steps to ensure Cyber Safety
- Charging and readiness of BYOx device
- Compliance with existing ICT Policy

The Responsibilities of the Parent/Caregiver

- Participation and encouragement of your student in the BYOx Program
- Care and maintenance of BYOx device
- Internet access and filtering when your student is not connected to the DOE network
- Protection of device using an adequate bag or carry case

Device Technical Issues

You are responsible for your BYOx device. The school is in no way liable for any damages that may occur to the device whilst at school. Any technical issues involving our network or systems will be rectified by our school ICT technicians. All issues relating to the device itself or any software not provided by the school are to be resolved by the student, parent/caregiver, or vendor. Our school technicians are not able to resolve these issues.

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.

Misuse and Breaches of Acceptable Usage

Students are advised that they will be held responsible for their actions while using the internet and online communication services. Students will be held responsible for any breaches caused by other users 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.

Use of the Department of Education Network and Internet Services

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

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

Communication through internet and online communication services must also comply with the department's Code of School Behaviour and the Student Code of Conduct available on the school website.

While on the school network, students shall 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.

Managed Internet Services and Internet Filtering

Internet access allows students to undertake and complete a range of activities and tasks. However, with the increasing number of users and uses of and on the internet, it has become increasing important to protect yourself for the ever-increasing number of malicious sites, users, and practices. The Department of Education has developed and implemented the use of managed internet services to deploy Internet filtering across all Queensland State Schools. All devices connected to the Department of Education networks will be subject to Internet filtering protecting them against malicious and inappropriate sites, spyware and malware, peer to peer sessions as well as scams and identity theft. However, it is impossible to eliminate one hundred percent of threats posed on the internet meaning any malicious or inappropriate sites that are not currently blocked by the filter must be reported to the school upon discovery. Please be aware networks outside of the Queensland Department of Education are not subject to web filtering and it is the parent or caregivers' responsibility to monitor a student's access to the internet outside of school.

Monitoring and Reporting

Students are advised 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.

Intellectual Property and Copyright

Students shall not plagiarise information and shall observe appropriate copyright clearance, including acknowledging the original author or source of any information, images, audio etc. used. It is also important that students 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

The school 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.

Students shall not possess, use, or distribute unlicensed or pirated software. All software installed on a student's device shall be obtained from the official site and or store. Failure to follow these precautions may result in a virus or other malicious software being present on the device and posing a threat to the user or network. Piracy shall not be committed by any student and pirated content is not to be used or stored on the school's network or devices.