MOUNT CROSBY STATE SCHOOL
STRONG AND SURE

BeConnected

Mount Crosby State School

BYOD Program

BeConnected at Mount Crosby State School

Overview

Over the past decade our students, as well as technology, have changed. These fundamental changes impact on what we teach and how students learn. It is therefore important to provide opportunities for students to develop the knowledge, skills and attitudes to prepare for a future in the 21st century. With students having 24/7 access to a digital device, learning will extend from the classroom to wide-reaching resources providing learning anywhere, anytime. With a powerful new tool set, students and teachers are able to engage in valuable new learning experiences. The **BeConnected at Mount Crosby State School** program has been established with a goal to facilitate a digital learning environment for every student in Years 3 - 5 at both school and home. We must provide students with the opportunity to be effective digital learners who become confident, creative and productive in a digital world.

What is BYOD

“Bring your own device (BYOD) refers to technology models where students bring a personally owned device to school for the purpose of learning. A personally owned device is a technological device brought into the school and owned by a student (or the student’s family), staff or guests” (Alberta Education, 2012). Put simply, BYOD is a solution where students quite literally bring their own device to school in order to access the Internet and/or school network through a managed Wi-Fi connection. There are various models for BYOD which can be adopted. In 2022 Mount Crosby State School will permit iPads meeting a certain specification to connect to the school’s wireless network to enable students to learn digitally. This may expand to include other devices pending infrastructure and future technology advancements.

BeConnected at Mount Crosby State School

In 2022 the approved device for Years 3-5 is an iPad. Students with BYO devices (iPads) will have access to a **filtered** Internet connection and classroom content. Students and parents/caregivers are asked to lend their support to this very valuable and innovative program. Strong support from parents and caregivers is paramount to ensuring the program is successful and that students gain maximum benefit for their learning.

Initial Wi-Fi Connection - BYOx Link

All devices must be set up at home before they can be used within the school. This procedure preloads the device with the wireless configuration so that the device will connect automatically when onsite. The following links contains videos on how to set up your child's device for use with the college. If you are unsure of your student's email address or password, then please contact their class teacher.

IPAD - BYOxLink - How to guide - iOS - Enrol your BYO device into Intune

https://mediasite.eq.edu.au/mediasite/Play/bbe46710d2c24274a0a99cba446a92031d

Minimum Device Specifications

In order to provide a consistent experience for students, it is important the device meets the minimum standards recommended by our school. This will ensure the device is able to connect to the school's network. This ensures that digital content used in the classroom is compatible with the chosen device. Please choose only the device that meets the specifications outlined within this document.

Purchasing a Device for BeConnected

The **BeConnected** program relies heavily on the desire for students to bring their devices to the college on a daily basis. It is a good idea to purchase the device early so the student can become familiar with it and hit the ground running when they start in the new year. Please read **BeConnected** section of our website to ensure your device meets the required specifications. This "live" section of the website allows us to provide updated information as devices are added to the compatibility list. When purchasing a device, it is important to consider future technical support requirements.

As part of the **BeConnected** Program, technical support is provided for connectivity issues in connecting BYO devices to the school network. We are unable to provide technical support beyond this. MCSS strongly recommends that families seek and provide their own warranty and insurance (accidental damage) protection for all BYO devices. MCSS cannot be responsible for any damage to the device. Please note that the school will take all reasonable steps to connect private devices however it cannot take any responsibility if it is unable to connect a particular device. Please investigate any tax rebate eligibility to ensure that you receive any credit to which you are entitled.

Case Requirements

All students are required to have a **robust** protective case for their device. For students with iPads, a case is required as well as a protective sleeve or pouch. The case must protect the iPad from damage in the event it is dropped. The iPad case should have a screen protector built in otherwise it will require a screen protector. An iPad sleeve or pouch goes over the case and is essential to protect the device when in transit in the school bag and should adequately protect and prevent the iPad from being exposed to the elements. Devices should always remain in their protective cases (and sleeve) during transport between classes and between school and home. When not in use they should also be in their protective case. Students are expected to have name labels placed on the following locations:

- A name label easily visible on the case of the device.
- A key tag for the protective sleeve/pouch/case for ease of identification.

App and Update Requirements

- App and update is the responsibility of the student/parents/caregivers.
- A core set of applications will need to be installed on each device as well as specific year level applications.
- A list will be provided at the end of each school year. It is critical that these applications are loaded onto the device before it is brought into the school. Without all applications present your child will not be able to operate effectively in class.
- If apps are missing the student may be advised to not bring the device again until they have been installed.
- It is important that all devices have at least 2GB free (as a recommendation) at all times to ensure that there are no issues associated with a lack of free space on the device.
- It is essential that students have created a passcode / password for their device and that this remains known to them only to ensure the security and safety of their device and their work.
- Students may install or have parents install other applications onto their device. Please remember that Apple do not permit students under the age of 13 to create an Apple account.
- Students may have games or other apps on their devices but they are not permitted to use these during school hours.
- We recommend that families make use of Apple’s Family Sharing and Screen Time features so that apps can be shared amongst siblings and so that parental controls can be established to limit screen time where appropriate.

- It is important that there is no illegally downloaded media or software on the device. Devices are never to be used to engage in illegal activity, including violation of copyright or other contracts.

Microsoft Office 365

A Microsoft Office 365 licence is available to all students at no cost. Microsoft Office 365 contains the products Word, Excel, PowerPoint, Outlook (desktop and online version), OneNote and access to OneDrive. Details on how to install, access and use can be found here: http://education.qld.gov.au/learningplace/help/home-computer-support.pdf

OneDrive

Sharing files

Students can only share files with people who have an @eq.edu.au email address. This includes staff and students.

To share a file, students will need to type the user's full @eq.edu.au email address. With regards to file sharing, students should:

- only share files with people that they know;
- edit the sharing permissions to 'Specific People', so only people with whom the link is shared can access the file.
- check they have entered the email address accurately before sharing;
- only open files that have been shared with them by someone they know; and
- alert their teacher if they think someone has accidentally shared a file with them, or someone has shared files that are not appropriate.

School vs Personal files

Students should only use OneDrive to share school related files. School related files include those that are created for the purpose of completing a class activity or an assignment. Students should ask themselves, 'would I get in trouble or be embarrassed if my teacher saw this file?' If the answer is 'yes', then it is likely that the file should not be stored in the student's OneDrive.

Examples of files **that would not be appropriate** to store in OneDrive, include:

- your personal journal or diary (excluding one written as part of a class activity or assignment)

- your contact list (e.g., yours or your friends' addresses, emails, phone numbers, photos etc.)
- account credentials (e.g., social media user names and passwords)
- personal photos and media (e.g., video or sounds files of you, your family and friends).
- Games (excluding school related projects)
- Your personal movie or television collection Students should check with their teacher/s if they're not sure whether a file should be stored in OneDrive.

Syncing files

Use of OneDrive can affect the school's internet speed. To avoid negative impacts, students should avoid:

- uploading large files, or large numbers of files to their OneDrive library during school hours
- inserting large images or attachments directly into OneNote Notebooks or Class Notebooks.

Enrolment status

When a student's enrolment status changes (e.g., following move to non-state school, Year 12 graduation), they will no longer be able to access their @eq.edu.au email or OneDrive library. Students must back up any files/emails they wish to keep prior to leaving the school.

MCSS Technical Support

School technician will assist students in the BYOD program with the connection of their device to the school network and any ongoing connection issues. Technical support is limited to:

- Connection of the device to the school wireless network
- Connection of the device to the school's printers

MCSS technician is not able to support students with (but not limited to):

- Hardware faults
- Software issues
- Physical damage to your device

- Issues caused by viruses – this is highly unlikely with Apple products. (It is important to note that where a device potentially threatens the school network, it may be temporarily or permanently suspended from connecting).
- Students are to contact their teacher if they require technical support or are experiencing any issues.

General Care and Acceptable Use

Students are responsible for the general care of their device.

Use and care of your device

- Bring your device to school each day fully charged.
- Hold your device with two hands when carrying it.
- It is recommended that food and drinks should not be next to your device when in use.
- Plugs, cords and cables should be inserted and removed carefully.
- Devices should be carried within their protective case where appropriate.
- Turn the device off before placing it in its bag.
- Devices should never be left unsupervised – unless locked in classroom or OSHC space.
- Students are responsible for ensuring the battery is **fully charged** for school each day
- Avoid dropping or bumping your device.
- Don't place technology devices in areas that may get very hot.
- Don't get devices wet. Even though they may dry and appear to operate normally, the circuitry could slowly corrode and pose a safety hazard.
- Follow all instructions given by staff.
- Avoid exposing your device to direct sunlight or sources of heat such as desk lamps, dust, dirt, rain, liquids or moisture, heavy shock or vibration.

Protecting the screen

- Carrying devices with the screen open should be avoided.
- Avoid poking at the screen — even a touch screen only requires a light touch.
- Do not place anything near the device that could put pressure on the screen.
- 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.
- Use a tempered glass screen protector.

Charging of Devices

Students generally do not have the opportunity to charge their device during class and it is expected that devices used within the school have sufficient battery power to last an entire day. The device is to be fully charged before the commencement of each school day. WH&S requirement limit the availability of access to charging stations within the school.

Mobile Data Networks (eg, 3G, 4G, 5G) and Internet Tethering

Mobile network tethering, wireless internet access points and inbuilt data connectivity can **provide students with an UNFILTERED network connection** within the school grounds. These types of internet connections **need to be disabled before arrival at school** as the school **cannot monitor or take responsibly for content accessed** via these methods.

Safety and Security

Students are responsible for the security and use of their device whilst at the school.

Security of Devices

Students are to remain with their devices at all times and they are only to be used in class with the support of your teacher. Students may take the sleeves/pouches containing devices into classrooms once their teacher has opened the classroom for the day. Students must otherwise stay with their bag and device. Under no circumstances should devices be left unsupervised.

Passwords

Each student at Mount Crosby State School has their own unique user account. Passwords must not be obvious or easily guessed. They must be kept confidential, and changed when prompted or when known by another user. Personal accounts cannot be shared. Students should not allow others to use their personal account for any reason. When using desktop computers, students should log off at the end of each session to ensure no one else can use their account.

Cybersafety

At any time, if a student believes they have received a computer virus or spam (unsolicited email), or they have received a message that is inappropriate or makes them feel uncomfortable, they must inform their teacher, parent and/or caregiver as soon as is possible. Students and parents are encouraged to explore and use the Government's e-safety website to understand, take appropriate precautions and learn how to deal with any cybersafety issues. You can find this information at the link below:

https://www.esafety.gov.au/

Parents are also encouraged to visit and explore the Government iParent website for guidance with using safety settings on your family's web-connected devices, tips for choosing movies and games and strategies for keeping young people safe online.

https://www.esafety.gov.au/parents

Students must 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 messages, 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 or publish:

- Unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments
- Sexually explicit or sexually suggestive material or correspondence
- False or defamatory information about a person or organisation.

Students must not engage in cyberbullying, which may include threats, bullying or harassment of another person. Cyberbullying, regardless of where it happens, will be dealt with in accordance with Education Queensland's Policies and incidents will be reported to the police where required.

Digital Communication Tools

We require that instant messaging and audio / video communication features **are not used within the school**, which includes but is not limited to Skype, Facebook, or iMessage. No attempts should be made to use such services on **BeConnected** devices within the school or whilst connected to the DET network.

Web Filtering

An internet filtering solution provides DET with the ability to restrict access to inappropriate material on DET's network. Content filtering is active only whilst the device is connected to the school's wireless network. To help keep students safe, **we do not permit students to use their own 3G or 4G mobile data connection whilst on school grounds**. Any content accessed in this manner will not be filtered. It is important to remember filtering systems are not foolproof and do not replace the need for care when students are online. Parents, caregivers and students are encouraged to visit the e-safety site above to learn more. Students must not use VPN software or similar to bypass or attempt to bypass filtering restrictions.

Privacy and Confidentiality

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. The student should not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. Students must not record, photograph or film any students or school personnel without the express permission of the supervising teacher. Identifying images, audio content and personal information must not be uploaded to the internet or leave the school (this information may be saved on the school server only). It should also be ensured that privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interest.

Intellectual Property and Copyright

Students should never plagiarise information and shall observe appropriate copyright clearance, including acknowledging the original author or source of any information 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.

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 all data. While at school, students are able to save data to their personal OneDrive account. They are also able to save data locally to the 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 external hard drive or “cloud” based storage. Students should also be aware that, in the event that any repairs need to be carried out, the contents of the device may be deleted when the device is repaired / replace by your products vendor.

Monitoring of Use

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, DET will comply with all legislative requirements.

Internet Use

Students are required to report any Internet site accessed that they consider to be inappropriate. Any suspected security breach involving students, users from other schools, or from outside the Queensland DET must also be reported to the school.

Damage or loss of equipment

Devices are used within the college at your own risk. It is important to ensure that devices are insured against theft, damage or loss in order to avoid unexpected expenses. Many home insurance policies allow you to specify coverage for mobile devices and we strongly recommend taking advantage of this. Any software or hardware issues, vandalism, damage, loss or theft of the device **must be reported immediately** to the school. Devices with dangerously cracked screens are not to be used within the school.

Daily Usage

Unless specifically advised otherwise by their teacher, students should bring their device every day. Devices will only be used when they are best fit for current learning outcomes. No other student will be permitted to nor should be using your child’s device within the school.

Before and After School Usage

Students **are not permitted to used their device on school grounds before or after school** without the express permission of a teacher and under their direct supervision. Devices are not to be removed from school bags until students are in their classroom and their teacher has directed them to do so.

Lunchtime Usage of iPads

Students **are not to use their device at lunch** unless arranged and supervised by a teacher.

Outside School Hours Care

Students who attend Outside Hours School Care should follow the directions of supervisors and follow all school procedures. Devices should only be used in designated areas for homework purposes if permitted to do so.

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 **misuse** of Internet and online communication services **may result in disciplinary action** which includes, but is not limited to, the withdrawal of access to services and/or device.

Mount Crosby State School ICT Responsible Use Policy

Upon enrolment at MCSS, all students and parents/caregivers are required to sign the *Mount Crosby State School ICT Responsible Use* Policy*.* This policy also forms part of this agreement. The Responsible Use Policy conditions apply to the use of the device and Internet both on and off the school grounds. Communication through the Internet and online communication services must also comply with the *Student Code of Conduct* which is available on the school website. There are a few conditions that students must adhere to, these include but are not limited to the following. 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
- share a mobile data network connection (e.g. 4G/5G) with themselves or others on school premises and will ensure that this feature is disabled prior to coming to school

- use unauthorised programs and intentionally download unauthorised software, images or music
- intentionally damage or disable computers, computer systems or Queensland DET 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 can be audited and traced to the account of the user

Period of Participation

Mount Crosby State School agrees to provide access to the student/caregiver from the date soon after this agreement is signed by all parties. The agreement may be ended earlier, at the school's absolute discretion, if:

- The student is no longer enrolled at the school

- The student is excluded from the school

- The parent and/or caregiver fails to comply with the BYOD Rules for Students, the school's ICT Responsible Use Policy or the Student Code of Conduct.

Contact Information

For all enquiries regarding this program, please contact:

Corey Ridden - Deputy Principal - Mount Crosby State School

Email: clunn@eq.edu.au - Phone: 07 3813 2222