Department of Education, Training and Employment

Student BYOD Charter

Maleny State High School

Version 4.0

Great state. Great opportunity.

Queensland Government

Contents

BYOD overview

Bring Your Own Device (BYOD) is a new pathway supporting the delivery of 21st century learning. It is a term used to describe a digital device ownership model where students or staff use their personally-owned laptop devices to access the department's information and communication (ICT) network.

Access to the department's ICT network is provided only if the mobile device meets the department's security requirements which, at a minimum, requires that anti-virus software has been installed, is running and is kept updated on the device Advice for State Schools on Acceptable use of ICT Facilities and Devices.

Students are responsible for the security, integrity, insurance and maintenance of their personal mobile devices and their private network accounts.

The department has carried out extensive BYOD research within Queensland state schools. The research built on and acknowledged the distance travelled in implementing 1-to-1 computer to student ratio classes across the state, and other major technology rollouts.

Maleny State High School has chosen to support the implementation of a BYOD model because:

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

Device selection

Before acquiring a device to use at school the parent or caregiver and student should be aware of the school's specification of appropriate device type, operating system requirements and software. Maleny State High School **does not recommend** a specific device however the following specifications should be met.

Laptop Operating System	**Version**
Apple	MAC OS X 10.6+
Windows	7 (and service packs)
Windows	8
Windows	8.1
Windows	10

The following operating systems are **incompatible** with this solution.

Operating System	**Version**
Windows	RT
Windows	Mobile (phone)
Linux	All
Unix	All
BSD	All
Google Chrome OS	All

Note: *Operating systems **must** have an antivirus product installed before being granted access to the school network.*

Operating System Compatibility Matrix

While both Mac OSX and Windows computers will connect to our BYO network and access internet services, the compatibility with our network, folder access and printing differs between operating systems. Below is a matrix that outlines the compatibility for each operating system.

IT Service	Apple OSX	WIN 7 (+SP)	WIN 8	WIN 8.1	WIN 10
Connect to BYO wireless network and access internet	✓	✓	✓	✓	✓
Connect to Curriculum Drive (resources)	✓	✓	✓	✓	✓
Connect to H Drive (student disk space)	✗	✓	✓	✓	✓
Be able to submit files to Submission Folders	✓	✓	✓	✓	✓
Connect to designated BYOD printer (basic printing)	✓	✓	✓	✓	✓
Print double sided documents	✗	✓	✓	✓	✓
Adjust print margins	✗	✓	✓	✓	✓
Select colour or black printing	✗	✓	✓	✓	✓
Select staple option	✗	✓	✓	✓	✓

Recommended Hardware & Software:

Due to current licensing agreements, Maleny State High School will work to ensure that Computer rooms/Workstations are provided for students enrolled in computer based subjects. i.e Graphics, Certificate I & II Information Digital Media and Technology, Junior Information Technology, Computing Application Technology. This will reduce the need for parents or care givers/students to purchase expensive devices. The following hardware and software specifications are advised when seeking devices for a BYOD Program.

Required Hardware:

- 1 x USB port (recommended)
- Mouse (touchpad) and keyboard
- 10” screen size or larger.
- 2 GB of RAM or higher
- Ethernet Port
- Wifi
- HDMI and/or VGA output
- Minimum 64GB Personal Storage (Internal Hard drive)

Software:

- Microsoft Office :- A free version of Microsoft Office 2016 is available to Education Queensland Students. Click here for instructions on how to download it or ask the School ICT Coordinator.
- Virus Protection – A discounted version of Norton Security is available to Education Queensland Students. Click here for instructions on how to download it or ask the School ICT Coordinator.
- PDF reader
- Media Player
- Internet Explorer or Firefox or Google Chrome
- Paint or similar program
- Devices running Mac OS X will also require the latest version of Java.

Accessories:

Cases should be purchased with devices. Hard padded cases can significantly reduce damage from any impact. Students must ensure they turn off a machine before they put it in a case to avoid overheating.

Common Questions and Answers:

Will every device work inside the Education Queensland network?

No. Some devices with low specifications have been found to not connect within the EQ network and may have difficulty with the security filters EQ uses.

Do I need 3G/4G?

The school has an effective wireless network available. It is EQ policy to use the web proxy. 3G/4G will assist devices that have non-wireless connectivity at home. 3G/4G enables UNFILTERED internet access at school. 3G/4G connections on BYOD devices must be turned off at school.

Who should be the administrator of the computer?

In order to connect to the BYOD wireless network, **students** must be a local administrator on their device.

What is the role of the school technician?

Maleny State High School's BYOD program does not include school technical support or charging of devices at school. The school technician will assist with the initial connection of the device to the school network, however they are not authorised to change settings on a machine without authorisation of the local administrator.

Can students bring their charger and charge their device at school?

No, students are unable to charge their device at school. **This is a logistical and workplace health and safety matter and is not negotiable**. Students must ensure that their device has at least 5 hours of battery life for the school day.

Printing

Students will be able to print via software that makes the printers available to personal devices. Printing at Maleny State High School is managed via a program called Papercut. At the start of each year student are automatically assigned $1 to their Papercut account. Students can assign more credit to their Papercut account in $5 increments.

Device care

The student is responsible for taking care of and securing the device and accessories in accordance with school policy and guidelines. Responsibility for loss or damage of a device at home, in transit or at school belongs to the student. Advice should be sought regarding inclusion in home and contents insurance policy or other warranties.

It is advised that accidental damage and warranty policies are discussed at point of purchase to minimise financial impact and disruption to learning should a device not be operational.

General precautions

- Food or drink should never be placed near the device.
- Plugs, cords and cables should be inserted and removed carefully.
- Devices should be carried within their protective case where appropriate.
- Carrying devices with the screen open should be avoided.
- Ensure the battery is fully charged each day.
- Turn the device off before placing it in its bag.

Protecting the screen

- Avoid poking at the screen — even a touch screen only requires a light touch.
- Don’t place pressure on the lid of the device when it is closed.
- Avoid placing anything on the keyboard before closing the lid.
- Avoid placing anything in the carry case that could press against the cover.
- Only clean the screen with a clean, soft, dry cloth or an anti-static cloth.
- Don’t clean the screen with a household cleaning product.

Data security and back-ups

Students must ensure they have a process of backing up data securely. Otherwise, should a hardware or software fault occur, assignments and the products of other class activities may be lost.

The student is responsible for the backup of all data. While at school, students may be able to save data to the school’s network, which is safeguarded by a scheduled backup solution. All files must be scanned using appropriate anti-virus software before being downloaded to the department's ICT network.

Students are also able to save data locally to their device for use away from the school network. The backup of this data is the responsibility of the student and should be backed-up on an external device, such as an external hard drive or USB drive.

Students should also be aware that, in the event that any repairs need to be carried out the service agents may not guarantee the security or retention of the data. For example, the contents of the device may be deleted and the storage media reformatted.

Common Questions and Answers:

Do I need some form of insurance for this device?

Yes, pilot schools have identified that most students will have their device damaged in some form over the course of a two year period. Some form of accidental damage policy is strongly recommended.

What happens if my device is stolen at school?

Students bringing their own device to school need to ensure they look after their device. Parents need to arrange adequate insurance in case of damage or theft. The school is **not liable** for any damage or theft that occurs on school property.

What warranty should I get with my device?

Some stores offer replacement warranties. Some offer an accidental damage policy. Other stores offer extended 3 year warranties. Some home & contents insurance are suitable. Check the conditions of insurance with the service vendor.

Acceptable personal mobile device use

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

This policy also forms part of this Student Laptop 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 Responsible Behaviour Plan available on the school website.

While on the school network, students should not:

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

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

Passwords

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

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

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

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

Students should also set a password for access to their BYOD device and keep it private.

Parents/caregivers may also choose to maintain a password on a personally-owned device for access to the device in the event their student forgets their password or if access is required for technical support. Some devices may support the use of parental controls with such use being the responsibility of the parent/caregiver.

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 also supports students by providing school related expectations, guidelines and consequences.

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 and Cyberbullying guide for parents and caregivers.

Web filtering

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

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

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

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

Students are required to report any internet site accessed that is considered inappropriate. Any suspected security breach involving students, users from other schools, or from outside the Queensland DETE network must also be reported to the school.

The personally-owned devices have access to home and other out of school internet services and those services may not include any internet filtering. Parents and caregivers are encouraged to install a local filtering application on the student's device for when they are connected in locations other than school. Parents/caregivers are responsible for appropriate internet use by students outside the school.

Parents, caregivers and students are also encouraged to visit the Australian Communications and Media Authority's CyberSmart website 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.

Software

Parents/caregivers may be required to install and support the appropriate use of the software in accordance with guidelines provided by the school. This includes the understanding that software may need to be removed from the device upon the cancellation of student enrolment, transfer or graduation.

Monitoring and reporting

Students should be aware that all use of internet and online communication services can be audited and traced to the account of the user.

All material on the device is subject to audit by authorised school staff. If at any stage there is a police request, the school may be required to provide the authorities with access to the device and personal holdings associated with its use.

Misuse and breaches of acceptable usage

Students should be aware that they are held responsible for their actions while using the internet and online communication services. Students will be held responsible for any breaches caused by other 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 and/or device.

Classroom disciplinary action

Teachers will give clear expectations on how the device will be used in their classroom. This may vary depending on the type of subject and classroom environment.

If the student chooses to disregard these expectations and/or are using their device in a way that **interferes** and **disrupts** with their own and other students' **learning** and **production** of **quality work**, the following process will be undertaken.

1. Teacher identifies irresponsible device usage that impacts upon the learning and production of quality work for the said student or other students.

2. The teacher reads the RTC questions to said student regarding their behaviour and usage of the device.

3. If student continues to be irresponsible with the device, the teacher will proceed through the normal RTC referral process.

4. Student will complete the RTC plan in preparation for his/her interview with the teacher and re-entry to the classroom.

If the student attends the RTC for device misuse 3 times throughout a semester, the school will;

1. Restrict/remove access of personally owned mobile devices to the intranet, internet, email or other network facilities for the **remainder of the semester.**
2. Temporarily suspend the students BYOD Charter for **the remainder of the semester**. The student will not be able to bring their device to school.

Repeated offences beyond the three RTC referrals will result in a meeting with the IT HOD and relevant Deputy Principal with the possibility of further disciplinary action.

Responsible use of BYOD

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 BYOD program:

School

- Onboarding to the network
- 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 BYOD Charter Agreement.

Student

- participation in onboarding (connection) process.
- acknowledgement that core purpose of device at school is for educational purposes
- care of device
- appropriate digital citizenship and online safety (for more details, see ACMA CyberSmart)
- 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 BYOD Charter Agreement.

Parents and caregivers

- acknowledgement that core purpose of device at school is for educational purposes
- internet filtering (when not connected to the school's network)
- encourage and support appropriate digital citizenship and cybersafety with students (for more details, see ACMA CyberSmart)
- 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 BYOD Charter Agreement.

Technical support

	Connection:	**Hardware:**	**Software:**
Parents and Caregivers	✓ (home-provided internet connection)	✓	✓
Students	✓	✓	✓
School	✓ school provided internet connection	x	✓ (some school-based software arrangements)
Device vendor	x	✓ (see specifics of warranty on purchase)	x
School Technician	✓ Will assist with device connect	x	x

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

- Use mobile devices for:
  - using the device solely for learning tasks/activities as directed by teaching staff.
  - 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 school work
  - 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 mobile device.
- Switch off and place out of sight the mobile device during classes, where these devices are not being used in a teacher directed activity to enhance learning.
- Use the personal mobile device for private use before or after school, or during recess and lunch breaks.
- Seek teacher's approval where they wish to use a mobile device under special circumstances.

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

- using the device in an unlawful manner
- using the device for the bulk transmission of unsolicited electronic mail
- 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 mobile device (including those with Bluetooth functionality) to cheat during exams or assessments
- take into or use mobile devices at exams or during class assessment unless expressly permitted by school staff.

In addition to this:

Information sent from our school network contributes to the community perception of the school. All students using our ICT facilities are encouraged to conduct themselves as positive ambassadors for our school.

- Students using the system must not at any time attempt to access other computer systems, accounts or unauthorised network drives or files or to access other people's devices without their permission and without them 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 BYOD program supports personally-owned mobile devices in terms of access to:

- Basic printing
- internet
- file access and storage (dependent on operating system)
- support to connect devices to the school network.

However, the school's BYOD 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.