Department of Education and Training

William Ross State High School

Bring Your Own Device (BYOD)

Policy

Version: 2016-11-21

Queensland
Government

Contents

Personally-owned laptop (BYOD) policy

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 mobile devices to access the department's information and communication (ICT) network.

These mobile devices are limited to laptops and PC tablet devices. 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 and staff are responsible for the security, integrity, insurance and maintenance of their personal mobile devices and their private network accounts.

The BYOD 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 BYOD represents more than a personally-owned mobile device; it also includes software, applications, connectivity or carriage service.

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.

We have 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 can assist students to improve their learning outcomes in a contemporary educational setting.
- assisting students to develop knowledge and skills necessary for the 21st Century workforce, including digital-age literacy, innovative and creative thinking, effective communication and high productivity.

Device selection

Before acquiring a device to use at school the parent or caregiver and student should be aware of our minimum specification of appropriate device type, operating system requirements and software. These specifications relate to the suitability of the device to enabling class activities, meeting student needs and promoting safe and secure access to the department's network.

The William Ross State High School BYOD program will initially support filtered internet access. Once a technical solution is finalised access to printers and network drives (Public and H drive) will be available while at school. However, the school's BYOD program does not include: storage or charging of devices, insurance or school technical support.

Minimum Hardware Specifications:

Device / Specification	Junior Secondary	Senior Secondary
Processor	i3	i5
RAM	2GB	4GB
Hard Drive HDD	32GB	32GB – 1TB
Screen Size - *minimum*	11"	13" *(11" is acceptable if not enrolled in FTV, Graphics, ITS or Business)*
Wireless networking ability	802.1 b/g/n	802.1 b/g/n
Internal Speakers	Yes	Yes
Audio and USB Ports	Yes. 1x USB, 1 x HDMI	Yes (2 or more USB / HDMI ports)
Web Camera	Optional	Yes (only used at teacher direction)
DVD player/burner	Optional	Yes
Battery life	6+ hours	6+ hours
Carry Case	strong, water resistant and sturdy	strong, water resistant and sturdy

Software Requirements:

Software	Specifications
Operating system	Windows 7 or higher, Mac OS X or later
Office Software	Office 365 FREE Download: Go to https://portal.office.com and then follow the onscreen prompts
Anti-virus	Current, commercial grade anti-virus software (installed & current via regular updates): Symantec Anti-virus software is available from: http://education.qld.gov.au/learningplace/
Insurance	Accidental Damage Protection ADP + recommend device is included on home/contents policy

NOTE:
Operating Systems NOT SUPPORTED in this BYOD initiative are **Windows XP**, **Vista** or **Lynx.**
In addition **Chrome Books and Android devices** are not supported/compatible with Education Queensland ICT infrastructure.

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 of the device in home and contents insurance policy (recommended).

It is advised that accidental damage and warranty policies are discussed at point of purchase with the retailer 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 ready for 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.
- Household cleaning products should NOT be used to clean the screen.

Data security and back-ups

Students must ensure they have a process of backing up data securely in multiple locations (BYOD device hard drive + another external storage device). 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 should save their data to the hard drive of their personally owned device. *Once a technical solution is finalised, students will also be able to backup / save data to their H drives on the school network.* All files must be scanned using appropriate anti-virus software before being downloaded to their device or 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.

Anti-virus software

To connect to the school's computer network, a device **must have** a current commercial grade anti-virus program installed, functioning correctly and updated regularly.

To assist parents, the Department of Education and Training has negotiated the following agreement with Symantec: Students are eligible to purchase discounted anti-virus software for personal use. For $9.99 (1 device, 1 year protection) or $29.99 (1 device, 3 years protection), students can purchase Norton Security with Backup.

The software can be used with Windows, Mac, Android or iOS devices. An internet connection is required for downloading the software. Terms and conditions apply to the use of the software. To find out additional details concerning this offer, students should navigate to the Learning Place (http://students.learningplace.eq.edu.au). Select the appropriate phase of learning and then click on the Exclusive Security option.

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 BYOD Policy at William Ross State High School. 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 school's 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.
- use their BYOD access privileges to enable unauthorized devices or other students access to the department's ICT infrastructure.
- use **3/4G and all other cellular connections on other devices** at school as this function, when activated, allows students to bypass the EQ internet security filters. The School will take no responsibility for the content accessed by students using their personally owned devices outside of the wireless network.

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 are encouraged to explore and use the 'Cybersafety Help button' to talk, report and learn about a range of cybersafety issues.

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 *Responsible Behaviour Plan* and any specific rules of the school. To help protect students (and staff) from malicious web activity and inappropriate websites, the school operates a comprehensive web filtering system. Any device connected to the internet through the school network will have filtering applied.

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

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

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

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

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

Parents, caregivers and students are also encouraged to visit the 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

MS Office Students involved in the trial should have a current version of MS Office installed on their device. This should include Word, Excel, PowerPoint and OneNote. MS Access would be desirable for students studying Business or Information Technology.

To assist parents, the Department of Education and Training has negotiated the following agreement with Microsoft: In 2016, all students are able to download a **free version of Microsoft Office 365**, to a personal computing device. The software will need to be downloaded using a student's internet access at home. It should be noted that the total download package may exceed 1Gb of data. A fast internet connection is recommended. Students will not be able to download the software from school.

For additional details concerning this offer, students should navigate to the Learning Place (http://students.learningplace.eq.edu.au). Select the appropriate phase of learning and then click on the **Free Student Advantage Microsoft Office 2013 Suite** option. Students will be required to enter their MIS Username and Password, to access the site.

Anti-virus software (we recommend Norton Security with Backup)

To connect to the school's computer network, a device must have a current **commercial grade anti-virus program** installed, functioning correctly and updated regularly.

To assist parents, the Department of Education and Training has negotiated the following agreement with Symantec: Students are eligible to purchase discounted anti-virus software for personal use. For $9.99 (1 device, 1 year protection) or $29.99 (1 device, 3 years protection), students can purchase Norton Security with Backup. The software can be used with Windows, Mac, Android or iOS devices. An internet connection is required for downloading the software. Terms and conditions apply to the use of the software.

To find out additional details concerning this offer, students should navigate to the Learning Place (http://students.learningplace.eq.edu.au). Select the appropriate phase of learning and then click on the Exclusive Security option.

Subject Software

Due to licencing conditions, school owned software cannot be installed on private devices. Some subjects may require students to download software from the internet. These programs are usually free, however will require an internet connection and must be downloaded at home. Note that the installation and maintenance of software on a student's personal device, is the responsibility of the student and their family.

Carry Case

It is highly recommended that a carry case be purchased for the student's device. The case should be strong, sturdy and at least water resistant. The case should also be clearly labelled with the student's name. It's also recommended that the student's name is engraved on the laptop and that the Make/Model and Serial Number of the device is included on all insurance documents.

Printing

Students will be able to print school related documents in the Resource Centre (C Block), once the technical solution is finalised.

Charging Of Device (Battery Power)

Students will not be able to charge their device on school grounds. The device used should have sufficient battery power to last an entire day (6 hours). When charging the device at home, the correct power adapter should be used, otherwise damage to the device may occur. Safety procedures should always be considered when charging electrical devices.

Wi-Fi Connection

Connection of private devices to the school's computer network will be via the school's Wi-Fi network. Users will be provided with the steps to complete this action during the BYOD Induction. A connection can only be made after school technicians modify the student's existing school computer account.

Data Backups

Technology can fail, be lost or stolen. It is extremely important that students have a backup plan in case things go wrong. Weekly backups are recommended and preferably daily if a student is working on assignments. Students are encouraged to copy their most important files to an external hard drive or USB memory stick. Students can use Windows Backup to do this automatically.

Security of Device

Devices are the sole responsibility of the family.

The school accepts no responsibility for the security or safety of the device. Teachers and staff will not store or look after a device on behalf of students. Should damage to the device occur whilst at school by another student/s, the school is not at liberty to provide parents with details about other students or provide contact details of the parents of students who may have been involved in the incident. William Ross State High School does not accept responsibility for damage, loss or theft of the BYOD device

Monitoring and reporting

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

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

Misuse and breaches of acceptable usage

Students should be aware that they are held responsible for their actions while using the internet and online communication services. Students will be held responsible for any breaches caused by other person(s) knowingly using their account to access internet and online communication services.

The school reserves the right to restrict/remove access of personally owned mobile devices to the intranet, internet, email or other network facilities to ensure the integrity and security of the network and to provide a safe working and learning environment for all network users. The misuse of personally owned mobile devices may result in disciplinary action which includes, but is not limited to, the withdrawal of access to school supplied services.

Responsible use of 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

- BYOD Policy — including information on (but not responsible for) connection, care of device at school, workplace health and safety, appropriate digital citizenship and cybersafety
- network connection at school
- internet filtering (when connected via the school's computer network)
- some technical support (please consult Technical support table below)
- some school-supplied software e.g. Adobe, Microsoft Office 365 …
- printing facilities
- school representative signing of BYOD Policy Agreement Form

Student

- participation in BYOD program
- acknowledgement that core purpose of BYOD 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 *(MUST be fully charged at home each day, ready for classroom use)*
- 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

- read the William Ross State High School BYOD Policy
- read and sign the BYOD Policy Agreement Form
- 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 Agreement Form

Technical support

	Connection:	Hardware:	Software:
Parents and Caregivers	✓ (home-provided internet connection)	✓	✓
Students	✓	✓	✓
School	✓ school provided internet connection	not provided by WRSHS	✓ (some school-based software arrangements)
Device vendor		✓ (see specifics of warranty on purchase)	

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

- Use BYOD devices for:
  - engagement in class work and assignments set by teachers
  - developing appropriate 21st Century knowledge, skills and behaviours
  - authoring text, artwork, audio and visual material for publication on the Intranet or Internet for educational purposes as supervised and approved by school staff
  - conducting general research for school activities and projects
  - communicating or collaborating with other students, teachers, parents, caregivers or experts as part of assigned school work
  - accessing online references such as dictionaries, encyclopedias, 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
- 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.
- sharing or enabling an unauthorised user (unapproved BYOD user/connection) access to school's ICT infrastructure
- bypassing the school's internet filters by using another personally owned 3/4G device

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 initial access to:

- internet
- email
- then subsequent access to:
  - printing (once technical solution is resolved)
  - 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.

William Ross State High School

BYOD Policy Agreement Form

This form must be signed and returned to the school office, before the device can be connected to the school network. Note both the parent/caregiver and student must have read the BYOD Policy and signed the agreement form.

In signing this form, I acknowledge that:

- I have read and understood the BYOD Policy and the WRSHS Responsible Behaviour Plan.
- I agree to abide by the guidelines outlined by both documents.
- I am aware that non-compliance or irresponsible behavior, as per the intent of the BYOD Policy, the Responsible Behaviour Plan and/or other relevant policies, will result in consequences relative to the behaviour.

Student name:		
PEC Class:	**Year level:**	**MIS-ID:**
Student's signature:		**Date:**
Parent/caregiver's name:		
Parent/caregiver signature:		**Date:**
DEVICE DETAILS		
Type of Device (circle)	Laptop	PC/Tablet
Brand:		
Model:		
Anti-virus program:		
Office-suite:		

Note that this agreement will be considered to continue as long as:

- the student remains enrolled at the school - the student is not excluded from the school
- the student meets the school's behaviour and educational expectations
- the student complies with the policies indicated in the BYOD Student Charter booklet and the department's Acceptable Computer Use and Internet Access Policy

Also note that should the student acquire a new/replacement BYOD device, this BYOD Agreement Form ***must be resubmitted****, providing the school with the updated device details. Failure to do so, will result in the new device being unable to connect to the school's ICT infrastructure. Other consequences may also apply.*

To participate in the 2017 BYOD initiative, please **sign & return this form** to the school office, by **Friday February 10th 2017**