Acceptable Usage Agreement
for
Bring Your Own Device (BYOD)
and
ICT Facilities and Devices

Version 20 July 2016

Contents

IMPORTANT: Version 20 July 2016
THIS IS A WORKING DOCUMENT AND MAY BE UPDATED THROUGHOUT THE YEAR.
Newest version will be available from the School website. A message will be communicated via the newsletter when amendments are made.

BYOD Transition Plan

Browns Plains State High School is transitioning to a Bring Your Own Device (BYOD) model, for computers and other personal electronic devices, due to the cessation of the National Secondary School Computer Fund (NSSCF).

In 2016
- Year 10, 11, 12 and specialty subjects (Graphics, IT, Media): majority of students should be bringing their own device by the end of the year.
- Year 7, 8 & 9: students may bring their own device however access to computers will be available within their subject areas

In 2017 – all students are expected to bring their own device to school.

Forward

This document contains all the information and agreement (contract) that need to be signed by all students and parents/carers. Each family should thoroughly read and understand the content and follow all procedures.

Introduction

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 include but are not limited to laptops, notepads, tablet devices, voice recording devices, games devices, USBs, DVDs, CDs and smart phones. 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.

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. Please be aware that it is more than a personally-owned mobile device; it also includes software, applications, connectivity or carriage service.

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 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 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.

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.

Software and Applications

Installation and maintenance of personal software is the responsibility of the family. Genuine versions of software need to be installed to ensure updates. Some subjects require the use of subject specific software, all of which have different licencing arrangements for private purchase. See **Curriculum Software Requirements** for software and application requirements.

Where student licences are available for software, the BPSHS technician will install software on personal devices.

Charging of devices

Students are be expected to bring a fully charged device to school each day. Check Device Specifications for battery life reference or consult your technical support. No charging is allowed at school due to workplace safety concerns and potential for accidental damage.

Wi-Fi

Approved devices that meet the outlined specifications will recognise the School Wi-Fi and students will be able to connect. Standard EQ internet security filters will screen usage and access. All devices to access the Wi-Fi must be supportive of a wireless bandwidth.

3G / 4G / All Other Cellular Connections

3/4G and all other cellular connections must be disabled in all devices used 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.

Printing

Students will be able to connect their approved BYOD device via their web browser to access printers.

Insurance, Accidental Damage Protection & Warranty

Families are strongly encouraged to have insurance and warranty on personal devices.

Repairs and Maintenance

All maintenance for the IT device, operating system, software and/or apps purchased by the family are the responsibility of the family. Families should ensure quick maintenance turnaround for student devices.

School Technical Support

The school provides a range of technical support to assist students with difficulties*. This is available from 8.30am in the mornings and 1st lunch in the technician's room located in the Communication building. Full support is provided for school provided devices. Limited support for BYOD may be available such as:

- assistance with connection to the school's wireless facilities
- installation of specialist software
- possible assistance to log a job with a portal company

Access to school devices and support is dependent on resource contributions being up to date at all times.

Cost to Families

The cost of the BYOD system is included in the Technology Levy which is a part of the School Fees. The contribution includes:

- Speciality subject requirements
- Maintenance and service of printer network systems, and print credit
- School technical support officer (connecting to the Wi-Fi service, installation of school licensed software, troubleshooting support, backup help and support)
- Software access and maintenance of licencing for BYOD for example Adobe

Device specifications

The school's BYOD program may support printing, filtered internet access, and file access and storage through the department's network while at school. However, the school's BYOD program does not include school technical support or charging of devices at school.

Before acquiring a device to use at school please read the following technical specifications. 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.

Specifications	Device MINIMUM Specifications	Device HIGH-END Specifications (e.g. required for IT/Media/Graphics)
Options	Purchasing a device with minimum specifications:	Purchasing a device with hi-end specifications:
CPU	Intel: Processor Core i3	Intel: Core i5
RAM	4 GB Minimum	8 GB Minimum
Graphics	Intel Built in Graphics acceptable	Dedicated Graphic Chip

Storage	256GB Hard Drive or 128 GB SSD Optical Drive optional	500GB Hard Drive or 256 GB SSD Optical Drive optional
Network	Wireless	Wireless
Screen Size	11 to 13 inch recommended, 1280 X 720 minimum resolution 11" minimum, 15" + sizes not recommended	13 to 15 inch recommended, 1280 X 720 minimum resolution 13" minimum, 15" + sizes not recommended
Battery Life	6 hour minimum battery life	6 hour minimum battery life
Operating System	Latest version preferred	Latest version preferred
Virus Protection	Any protection accepted as along as it is a full up-to-date version NOT a trial version	Any protection accepted as along as it is a full up-to-date version NOT a trial version

Curriculum Software Requirements

ALL SUBJECTS – CORE SOFTWARE		
Function of Software	**Examples for Windows devices**	**Examples for Mac devices**
Word Processing	Microsoft Word 2013 or newer (Office 365)	Office 365
Spread Sheeting	Microsoft Excel 2013 or newer (Office 365)	Office 365
Presentation	Microsoft PowerPoint 2013 or newer (Office 365)	Office 365
Media/Video player	Windows Media Player, VLC Player	VLC Player
Photo viewer/manipulator	Microsoft Office Picture Manager, Adobe Photoshop, Paint.net	Adobe Photoshop
Internet browser	Internet Explorer, Google Chrome, Mozilla Firefox	Safari, Google Chrome
PDF creator & reader	Adobe Reader, Adobe Creator	Adobe Reader, Adobe Creator

SUBJECT SPECIFIC SOFTWARE				
	Subject	**Specific Software**	**Function**	**Software Access**
All Devices	Accounting	MYOB	Specific Accounting	MYOB student edition $15.00
	Art	Adobe Photoshop	Image Editing	Free with Base Adobe Package
	Business	MYOB	Specific Accounting	MYOB student edition $15.00
	IT (9 & 10)	Adobe Flash	Animation Software	Free with Base Adobe Package
		Adobe Photoshop	Image Editing	Free with Base Adobe Package
		Lego Mindstorm	Robotic Software	Free – See subject teacher for details
		Game Maker	Programming Language	Free – See subject teacher for details
	Music	Mixcraft 7	Music Composition	School access provided only.
		Ableton Live (Lite) Ignite	Music recording and editing	School access provided only.
		Audacity, A	Music recording and editing	Free
	PE	Swinger	Biomechanical analysis	School access only.
Device with high-end specifications	Graphics	Autodesk	Industry Standard	Free – See subject teacher for details
		Adobe Photoshop	Image Editing	Free with Base Adobe Package
	Media	Adobe Premiere	Film Editing	Adobe Master Collection $20.00
		Adobe Photoshop	Image Editing	Free with Base Adobe Package
	IT (11 & 12)	Blender	3D graphic generator	Free – See subject teacher for details
		Adobe Premiere	Film Editing	Adobe Master Collection $20.00
		Adobe Photoshop	Image Editing	Free with Base Adobe Package
		Lego Mindstorm	Robotic Software	Free – See subject teacher for details
		Unity + Game Maker	Programming Languages	Free – See subject teacher for details

Responsible Use

Upon enrolment in a Queensland Government school, parent/carer permission is sought to give the student(s) access to the internet, based upon the policy contained this acceptable usage agreement.

The responsible-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 this usage agreement and Responsible Behaviour Plan.

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).
- 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/carers 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/carers 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, carers 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/carers are encouraged to install a local filtering application on the student's device for when they are connected in locations other than school. Parents/cares are responsible for appropriate internet use by students outside the school.

Parents, carers 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.

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.

Acceptable Usage of BYOD and ICT Facilities & Devices

This document defines the acceptable use of BYOD and ICT Facilities & Devices for student use at Browns Plains State High School. Our goal is to ensure the safe and responsible use of facilities, services and resources available to students through the provision of clear guidelines.

Authorisation and controls

The principal (or delegate) reserves the right to restrict student access to BYOD and/or the school's ICT facilities and devices if access and usage requirements are not met or are breached. However restricted access will not disrupt the provision of the student's educational program.

The department and Browns Plains High School monitors access to and usage of their ICT network. For example, email monitoring will occur to identify inappropriate use, protect system security and maintain system performance in determining compliance with state and departmental policy.

The department and Browns Plains High School may conduct security audits and scans, and restrict or deny access to the department's ICT network by any personal mobile device, if there is any suspicion that the integrity of the network might be at risk.

Responsibilities for using the school's ICT facilities and devices

- Students are expected to demonstrate safe, lawful and ethical behaviour when using the school's ICT network as outlined in the *Browns Plains High School Responsible Behaviour Plan and this Usage Agreement*.
- Students are to be aware of occupational health and safety issues when using computers and other learning devices.
- Parents/carers are also responsible for ensuring students understand the school's ICT access and usage requirements, including the acceptable and unacceptable behaviour requirements.
- Parents/carers are responsible for appropriate internet use by students outside the school environment when using a school owned or provided mobile device.
- 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).
- Students cannot use another student or staff member's username or password to access the school network, 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 (e.g. name, parent's name, address, phone numbers), via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school.
- Students need to understand that 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.

Responsibilities of stakeholders involved in the BYOD program:

School

- BYOD program induction — 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 (refer to school technical support)
- some school-supplied software e.g. Adobe, Microsoft Office 365 …
- printing facilities

Student

- participation in BYOD program induction
- acknowledgement that core purpose of device at school is for educational purposes and the use of the device is at the discretion of the classroom teacher
- 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)
- 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 this User Agreement.

Parents and caregivers
- participation in BYOD program induction
- 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)
- technical support (refer to service agreement at time of purchase)
- required software, including sufficient anti-virus software
- protective backpack or case for the device
- adequate warranty and insurance of the device
- understanding and signing this User Agreement.

The following are examples of responsible use of devices by students:
- use 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, 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.
- 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.

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/carers need to be aware that damage to devices owned by the school, other students or staff may result in significant consequences in relation to breaches of expectations and guidelines in the school's Responsible Behaviour Plan.
- students who use a facility and/or device in a manner that is not appropriate may be subject to disciplinary action by the school, which could include but not limited to restricting network access and payment for repairs/replacement
- 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:
- printing
- internet
- file access and storage
- 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.
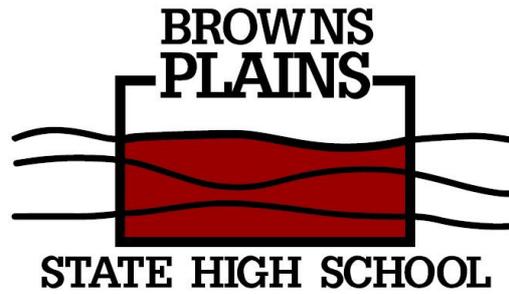
Acceptable Usage Agreement
for
Bring Your Own Device (BYOD)
and
ICT Facilities and Devices

Read the *Acceptable Usage Agreement for Bring Your Own Device (BYOD) and ICT Facilities and Devices* policy. The following is to be completed by both the STUDENT and PARENT/CARER:

- We have read and understood the *Acceptable Usage Agreement for BYOD and ICT Facilities & Devices* and the *Browns Plains SHS Responsible Behaviour Plan for Students.*
- We agree to abide by the guidelines outlined by both documents.
- We are aware that non-compliance or irresponsible behaviour, as per the intent of this Usage Agreement and the Responsible Behaviour Plan for Students, will result in consequences relative to the behaviour.

Student's name: ....… **Year:** .... **Username:** ....…….…….....
(Please print)

Student's signature: .....……..…………...Date: /   /

Parent's/caregiver's name:..…………………………................
(Please print)

Parent's/caregiver's signature: ....…………………...............Date: /   /