More information on Bring Your Own Device (BYOD)

manypathways No limits
Benowa STATE HIGH

What is BYOD?

BYOD stands for Bring Your Own Device. This model allows students to bring an IT device to Benowa SHS that best supports their learning needs (within specifications).

Benowa State High School is committed to moving students and staff forward in a contemporary learning environment.

IT devices are a powerful means of differentiating and personalising a student's education, and student-owned devices facilitate student choice over which application best suits their learning and communication style.

Teachers will work with students to ensure everyone can access and view a student's final work in appropriate formats as necessary.

We are giving families control over the choice of IT device to bring to school as their primary device (within specifications). With this primary device we will continue to support students by diagnosing IT issues and consulting with families if further action is required. We make the following recommendations around device specifications and software that students bring to school.

Subject Specific Software

Accounting

MYOB Education Edition

Multi Media / ITD

Adobe Master Collection Creative Cloud

Instrumental Music

Sibelius
Smart Music

Maths C –Maths Cad

Students in Maths C will require Maths Cad software. We are currently looking at licencing arrangements and whether educational pricing will become available.

Music / Music Industry

Sibelius - MuseScore - Ableton - Fruity Loops - Abelton - Krystal audio engine - Audacity

Photography

Students will require the Adobe master collection please see below about purchasing a licence through the school.

Visual Art

Photoshop

Graphics

Students choosing Graphics or Senior Engineering subjects will require a device that has higher capabilities than the minimum specifications stated above so that software can be run adequately.

Graphics students will use **Inventor, AutoCad** and **Archicad** as core programs. They will also require **Microsoft Office** programs installed. Graphics involves designing and students will also use **Photoshop** and **Illustrator**. Other programs for designing such as **Sketch Up** would be helpful but not critical.

System Requirements for Autodesk Inventor 2017:

Operating System:
64-bit Microsoft Windows 10

CPU Type Minimum:
Intel® Core i5 or AMD dual core 2 GHz or higher

Memory :
8 GB RAM or higher

Hard Drive Size :
256 GB or higher

Graphics Recommended:
Microsoft® Direct3D 11® or capable graphics card or higher [5]

Printing

Students will be able to connect their approved BYOD device via Papercut for printing.

Backing Up

As we all know, technology can fail and can be lost or stolen so it is extremely important that students have a backup plan in case things go wrong.

Backing up is easy. Once set up, your data should be backing up automatically. You just need to check every once in a while to make sure your backups actually work. There are two main types of backup solutions:

Local Backup

Every week, copy your most important files onto an external hard drive next to your desk, in your cupboard, or any other place where you can easily retrieve it. You can even use Windows Backup to do this automatically.

Offsite Backup

This is another automatic backup or an external hard drive that's stored at another location, such as a friend or family's house. This protects your backup in case of theft, natural disaster or simple hardware failure.

Care of Device

It is the responsibility of families to keep their chosen IT device in good working order to ensure minimal disruption to learning.

It is expected that students bring their IT device to school each day fully charged. Each device should be clearly labelled with the student's name.

Students should take care to put their device to sleep when moving around, as failure to do so can damage the Hard Drive and potentially lose files. Choosing a device with a solid state drive (SSD) can alleviate some of these issues.

Case / Carry Bag

A strong carry case is a great way to protect your device from accidental damage like drops. If you are needing to purchase a carry case or back pack with suitable padding for your device check out the HP and Dell Benowa SHS BYOD portals www.hpshopping.com.au/eduqld and https://myschoolshop.qld.datacom.com.au/benowashs

Access Key – benowashs
PIN – benowashs

Insurance

Purchasing insurance is a personal choice.

When purchasing your laptop please learn about your options to purchase accidental damage protection for your device. This covers your device with accidental damage, on and off the school campus. Fire, theft and Acts of God are usually not covered under these programs and we request you to include it in your personal or home insurance. The insurance can be purchased with your computer vendor or any insurance company. All insurance claims must be settled between you and the insurance company. Statistically, 30% of repairs at Benowa SHS are considered non-warranty. eg. Repairing a cracked screen from a drop can cost up to $1000.

Warranty

Devices purchased through the portals can be covered by a 3-year warranty, along with on-site repairs.

Devices purchased through an external provider (not through the portal) are not covered by any warranty with us. Please discuss warranty options with the provider you purchase from.

On average 70% of these repairs are warranty and 30% non-warranty.

School Support

If a student runs into a problem with their BYOD device, we advise students to see Benowa SHS IT staff who will attempt to diagnose the fault. If this is not able to be resolved by IT staff, they can recommend a course of action for repair (eg. warranty claim, insurance claim etc.)

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 School's Responsible Behaviour Plan both of which are 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.

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 *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.

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 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 (please consult Technical support table below)
- some school-supplied software e.g. Adobe, Microsoft Office 365 (anything that appears on the installation menu, which can be seen on the BYOD pamphlet)
- printing facilities
- school representative signing of BYOD Charter Agreement.

Student

- participation in BYOD program induction
- 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	✓ (dependent on school-based hardware arrangements)	✓ (some school-based software arrangements)
Devices purchased through the portal	✓	✓ (see specifics of warranty on purchase)	✓

Examples of responsible use of devices by students:

- Use mobile 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.
- 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.

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 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:

- 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

Further questions

If you have further questions which we have not answered in this document or on the brochure, please contact us directly at BYOD@benowashs.eq.edu.au. We will respond to you at our earliest convenience.