



Bring Your Own Device (BYOD)

Information for Students and Parents

Handbook 2016



Contents

Personally-owned mobile device charter	3
Forward	3
BYOD overview	3
Device selection	4
Software	5
Printing	5
Charging of devices	5
Wi-Fi and 3/4G	5
Secondary Device	5
Cost to Families	6
Responsibilities.....	6
Device care	7
Warranty.....	7
Data security and back-ups	8
Technical Support	8
Passwords.....	9
Digital citizenship	10
Cybersafety	10
Web filtering	11
Privacy and confidentiality.....	11
Intellectual property and copyright.....	12
Monitoring and reporting	12
Misuse and breaches of acceptable usage.....	12
Responsible use of BYOD	13
Responsible use agreement	16

Personally-owned mobile device charter

Forward

This BYOD handbook has been developed as a guide for parents and students about matters relating to the Bring Your Own Device BYOD program at Gympie State High School. Whilst you are not obligated to provide a BYOD digital device, each family who does decide to enter into a BYOD arrangement should thoroughly understand the content of this handbook and follow all procedures.

Gympie SHS understands that students engage with a wide variety of devices both inside and outside the school environment. The desired culture at Gympie SHS is where students engage effortlessly with contemporary teaching and learning practices. As a result, we aim to develop an environment where digital technology augments strong teaching and learning practices within the framework of our guiding principles.

With BYOD becoming available to students at Gympie SHS in 2016, teachers as life-long learners will continue to focus on their curriculum and balance their pedagogical skills to best utilise ICT in an educationally purposeful way. ICT in a contemporary world is being reflected in classrooms. The emphasis is upon students having the opportunity to access digital technology and incorporate the advantage of this into their learning. It is always to be remembered that digital technology is a tool for learning, actual learning is your student engaging with content and mastering skills in a meaningful and effective manner.

BYOD overview

Gympie SHS has a strong history of ICT integration, with the Laptop and iLearn programs leading the way. Bring Your Own 'x' (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 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, tablet devices, voice recording devices (whether or not integrated with a mobile phone or MP3 player), games devices (e.g. PSPs, Game Boys), 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 [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 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 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, it is essential that you are aware of the specification of appropriate device type, operating system requirements and software. These details are listed in the table below. Whilst other devices exist on the market which do not meet these specifications and which can be used to perform activities like connecting to the Internet and typing an assignment, they are not seen as providing an optimal learning experience.

These specifications relate to the suitability of the “Primary BYOD Device” to enabling class activities, meeting student needs and promoting safe and secure access to the department’s network. Should you have any specific questions in regards to a particular device please consult our IT staff and they will be happy to assist you.

Specifications	Minimum Level	High End Level
Screen Size	11" minimum 13 to 15 inch recommended 1280 X 720 minimum resolution	15 inch recommended 1280 X 720 minimum resolution
CPU	Intel Core i3 4th gen. or higher	Intel: Core i7
RAM	4 GB Minimum	8 GB Minimum
Storage	320GB Hard Drive 5400RPM	320GB Hard Drive 7200 RPM
Battery Life	4.5 hour minimum battery life	4.5 hour minimum battery life
Wireless	802.11g or higher	802.11g or higher
Operating System	Windows 7 and newer <i>NOT SUPPORTED: iOS, Android, Windows RT, Chromebook & distributions of Linux (eg. Ubuntu, Debian, Fedora etc.)</i>	Windows 7 and newer
Additional Features	Keyboard, USB port, headphone port, In-built microphone,	Keyboard, USB port, headphone port, In-built microphone, webcam

The school’s BYOD program supports 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.

Software

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 subject specific software, all of which have different licencing agreements for private purchases. Teachers of those subjects will advise which software is required when students join that subject.

Note that when purchasing a BYOD device, it is a requirement to purchase and install an Operating System, but NOT a requirement to purchase an Office package. Every student across Queensland will receive a copy of Microsoft Office365 Student Advantage. The base package is free and a more comprehensive package is available at a minimal cost. Students who want the free software will need an active Managed Internet Service (MIS) login, school email account and password. Those who don't have these should contact Mr Mayfield in H Middle Staffroom for assistance, who will help students activate their MIS login and provide a procedural document on how to obtain this software.

Technical support for managing software once it is installed onto the device will not be provided by the school. Installation and maintenance of personal software is the responsibility of the family, including the provision and installation of current and up to date antivirus software.

Printing

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

Charging of devices

Student will be expected to bring a fully charged to device to school each day. Check Device Specifications for battery life reference or consult your technical support.

Wi-Fi and 3/4G

Approved devices that meet the outlined specifications will recognise the Gympie SHS Wi-Fi network and students will be able to connect via a procedural document provided. Standard EQ internet security filters will screen usage and access. Students will be supported in connecting their device to the school wireless network.

3/4G ability must be disabled in all devices when connected to the Gympie SHS Wi-Fi network, as this function when activated allows students to bypass the EQ internet security filters. Gympie High will take no responsibility for the content accessed by students using 3/4G facility on their personally owned devices.

Secondary Device

Gympie SHS acknowledge that many of today's students interact with information and media on a variety of screens including computers, laptops, smartphones and tablets. Students are welcome to bring a secondary device, which is to be used in accordance with the ICT Responsible Use Policy (RUP) and the Acceptable personal mobile device use policy documents.

Cost to Families

There will be a cost of \$50 for entering the Bring Your Own Device program, which is payable at the Finance window. Once this has been paid and the attached “Responsible Use Agreement” signed and returned, students will be able to commence the process of getting their device connected to the schools network. The details of what is included for this cost are as follows:

- Technical ‘Help Desk’ support for all connectivity issues
- Secondary device Wi-Fi connection
- Upgrade and maintenance of wireless network infrastructure, servers and printers
- Software access and maintenance of licencing for BYO devices including:
 - GSHS Online Learning Server providing*
 - Digital curriculum content,
 - Online assessment submission
 - Clickview Online providing*
 - 24/7 access to resource library of educational videos through any computer or mobile device,
 - OLIVER V5 providing:*
 - 24/7 access to the entire College collection of print, electronic and AV resources on any mobile digital device
 - Federated searching across databases, websites, eBooks and AV resources

Responsibilities...

... of Gympie SHS	... of the Parent/s	... of the Student
<ul style="list-style-type: none"> • provide suitable school Wi-Fi connection and filtering system • provide a blended educational environment • model safe device and internet practices • provide access to GSHS Online Learning Server, Clickview Online and Oliver 	<ul style="list-style-type: none"> • provide a suitable device • maintenance of device • purchase, install and update software applications including antivirus software • appropriate insurance and warranty 	<ul style="list-style-type: none"> • bring device fully charged each day • show respect for other devices, work and privacy • access technology as a Responsible User

Device care

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. Any BYOD 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. 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.

Warranty

We advise that all devices are covered by an extended warranty to last the students' time at Gympie SHS. Statistically a computer will require, on average, 2.5 repairs during its 3 year life cycle. This is a computer requiring a hardware repair due to component failure (warranty) or accidental damage (non-warranty). On average 70% of these repairs are warranty and 30% non-warranty.

Data security and back-ups

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. 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 can and should 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.

Technical Support

If students experience a problem connecting to the school Wi-Fi network, they can seek assistance from Mr Mayfield in H Middle Staffroom. Software maintenance is the responsibility of the student and their family, and any hardware maintenance is the responsibility of the owner of the device and the vendor from whom it was purchased. No hardware or software maintenance will be provided by the school beyond providing connectivity support.

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 Personally-owned mobile device 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 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)
- connectivity technical support
- Ed Qld supplied software e.g. Microsoft Office 365
- 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 must not share their username and password)
- hardware and software technical support in conjunction with parents and the device vendor
- 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

- 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](#))
- hardware and software technical support in conjunction with the device vendor
- 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.

The following are 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.

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 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.

Responsible use agreement

The following is to be read and completed by both the **STUDENT** and **PARENT/CAREGIVER**:

- I have read and understood the BYOD Charter and the school 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 Charter and the Responsible Behaviour Plan, will result in consequences relative to the behaviour.

Student's name: **Year:** **ID No**
 (Please print)

Student's signature: **Date:** / /

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

Parent's/caregiver's signature: **Date:** / /