Department of Education and Training

# BYOD Handbook & Agreement

## for Students and Parents

Gympie State High School

Queensland
Government

## Contents

# Personally-owned mobile device agreement

## BYOD overview

Bring Your Own Device (BYOD) is an initiative to support the delivery of lessons in a 21st century context. It means students use their personally-owned mobile device (usually a laptop) to access the department's information and communication (ICT) network. In the modern era of education it is recognised that knowledge and ideas contribute to our nation's economic growth and we want to maximise the potential for your child to be a part of this growth. Students will use their device to collaborate and create, engage in lesson activities, conduct research, submit work and interact with teachers and other students.

Access to the department's ICT network is provided after the device has met the department's security requirements which, at a minimum, requires that anti-virus software (*see Support and FAQ page on school website*) has been installed, is active and is kept updated. This link, and all other links referenced in this document are available on the school website under **Quicklinks** on the "Advice for Parents - BYOD" page. Note that Microsoft Windows Defender is a free anti-virus package provided with Windows 10. Windows Defender is suitable for this purpose.

Benefits of the BYOD model are:

- Assists students in improving their learning outcomes; learning about being a responsible digital citizen; and encourages the development of skills that prepare students for future study and career paths.
- Supports learning at any time and place that is convenient for students.

Here are the recommended steps to acquire a device for your child:

1. Read this handbook and other BYOD information on the school website
2. Read "*Before you buy a new laptop for school*" section on the Support & FAQ page
3. Print the BYOD specification sheet to refer to when shopping
4. Compare deals from the purchase portal and other laptop suppliers
5. Confirm warranty and accidental damage cover are included in the price and that the return processes are convenient and cost-effective for you.
6. Some suppliers offer "Next Business Day" warranty service at the school with no need to send your laptop away for repairs. Contact byod@gympieshs.eq.edu.au for details.
7. Once you receive your laptop, connect it to the school's wireless network prior to first bringing the laptop to school. This can done from home by following the steps shown in the documents and videos found on our website by clicking on "Enrol your BYO device from home"

## Device selection & specifications

Before acquiring a device to use at school parents, caregivers and students should refer to the school's minimum device specifications. The specifications relate to the capability of the device and have been set based on normal operating requirements, class activities, meeting student needs and promoting safe and secure access to the department's network.

The school's BYOD system also supports printing, filtered internet access, and file access and storage through the department's network while at school. We're not able to guarantee access to charging facilities at school. Some classroom and resource spaces offer limited access for recharging devices; however it is recommended that battery life for your chosen device meet or exceed the minimum specification.

## Device care, damage, loss or theft

The student is responsible for taking care of and securing the device and accessories in accordance with school policies and guidelines. Responsibility for loss of or damage to the device, regardless of the location, rests with the student. Advice should be sought from your insurance provider regarding inclusion in your contents insurance policy.

It is advised that you discuss accidental damage cover and warranty policies at the point of purchase to minimise financial impact and disruption to learning should a device suffer from a malfunction or be lost or damaged. Some suppliers offer a three year accidental damage and loss policy. Refer to the purchase portal for more details.

### General precautions and operating principles

- Food or drink should not be consumed near the device.
- Plugs, cords, cables and accessories should be inserted and removed carefully.
- Devices should be carried within their protective case where appropriate.
- Carrying laptops with the screen open may lead to significant damage.
- Ensure the battery is fully charged prior to coming to school each day.
- Turn off the device or use hibernation mode before placing it in its case to prevent overheating.

### Protecting the screen

- Avoid poking at the screen. Even touch-screens require only a gentle touch.
- Don't place pressure on the lid (back of screen) when it is closed.
- Avoid leaving anything (such as USBs) on the keyboard before closing the lid as this can damage the screen.
- Avoid placing anything in the carry case that could press unevenly against the lid.
- Only clean the screen with a clean, soft, dry cloth or an appropriate anti-static cloth.
- Don't use household cleaning products on laptops.

## Data security and back-ups

Students are responsible for the integrity of their files and are strongly encouraged to adopt a suitable backup process for doing this. Otherwise, should a hardware or software fault occur, students may lose their work.

While at school, students are encouraged to save their work to the school's network, which is subject to a regular backup process such as a USB stick or external hard drive left at home.

Students can also save files on their device, or to their OneDrive account (www.office.com), for use away from the school network.

In the event that repair work is needed, the service agent may have to wipe data on the hard drive. The contents of the device may be deleted and the hard drive reformatted. In any case, it's a good idea to back up your files regularly.

# Acceptable personal mobile device use

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

The policy referred to above forms part of this Agreement. The acceptable use conditions apply to the use of the device, school network and internet while on school premises, and at any time the student is using their school account to access various services (email, OneDrive, etc.).

Communication through internet and online communication services must also comply with school rules and policies, which are available on the school website.

While on the school network, students should not:

- Create, access or circulate files or other 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 by the Department.
- Use unauthorised programs or intentionally download unlicensed media/content/software.
- Intentionally damage or disable computers, computer systems, printers, network devices, the school or government networks.
- Use the device for unauthorised commercial activities, lobbying, gambling or any unlawful purpose.

Note: Students' use of internet and online communication services, associated with their school account, 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 other students). IT Technicians may require your password to perform maintenance and repairs.

The password should be changed regularly, as well as when prompted by the department or when it may have become known by another person.

School network account credentials are not to be shared. Students should not allow others to use their account for any reason. Students are responsible for all actions taken using their account credentials. Students should log off, or lock their screen, at the end of each session to ensure no one else can use their account or device.

If available, students should also set an extra level of password protection for access to their BYOD device. This could be in the form of a boot-up password or other lock screen.

Parents/caregivers may also choose to maintain an administrator account 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 in the broader community.

Parents are requested to ensure that their child understands this responsibility and expectation. The school rules and policies also support 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 (on school computers) to report the matter 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 any computer;
- chain letters or hoax emails;
- spam (such as unsolicited advertising).

Students must never send, post or publish:

- inappropriate or unlawful content or that which is offensive, abusive or discriminatory;

- threats, bullying or harassment of another person;
- sexually explicit or sexually suggestive content or materials;
- 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. See link on website titled "Online Awareness".

## Web filtering

The internet has become a powerful medium for supporting teaching and learning; however, students need to be careful and vigilant regarding some web content. Students are required to act in line with all the normal school behaviour policies and expectations. To help protect the school community from malicious and inappropriate websites, the school utilises a web-filtering system. Any device connected to the internet through the school network will have this filtering applied.

The filtering system provides a layer of protection against:

- access to inappropriate web pages and content;
- spyware and malware;
- peer-to-peer file sharing;
- scams and identity theft.

This web-filtering solution takes a precautionary approach to blocking websites, including those that do not disclose information about their purpose and content. The filtering system employs best-practice techniques; however, despite precautions to manage inappropriate content on the internet, illegal, dangerous or offensive information may be unintentionally 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 or online content that is considered inappropriate. Any suspected security breach involving students, users from other schools, or from outside the school 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 filtering application on the student's device for when they are accessing online content other than at school. Parents/caregivers are responsible for appropriate internet use by their child at any time they're not using the school network.

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 engage with 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 private file space, 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 another person 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 (copy without proper attribution) and should observe appropriate copyright conditions, 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 in any form. 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 and be subject to prosecution from agencies that enforce such copyrights.

## Software

The school may recommend software applications, or supply download links, in order to meet the curriculum needs of particular subjects. Parents/caregivers may be required to install and support the appropriate use of the software in accordance with guidelines provided by the school. This includes the understanding that software may need to be removed from the device upon the cancellation of student enrolment, transfer or graduation.

As a bonus provided to all state school students, Microsoft have made Office 365 software available for free. Refer to the Microsoft free software link on the school website for details. This package includes Word, Excel, PowerPoint and several other programs. Don't pay extra for Microsoft Office when purchasing a BYOD laptop.

## Monitoring and reporting

Students should be aware that usage of internet and online communication services can be audited and traced to the account of the user. All Internet browsing history is stored in archives.

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

## 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 any other person who was knowingly given access to the student's account.

The school reserves the right to restrict or revoke access 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 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.

**Responsibilities of stakeholders involved in the BYOD program:**

***School***

- BYOD program induction — including information on connection, care of device at school, workplace health and safety, appropriate digital citizenship and online safety.
- Internet filtering (when connected via the school's computer network).
- Some technical support. Please refer to Support and FAQ on the school website.
- Some school-supplied software, subject to course enrolments.
- Printing, copying and scanning facilities.

***Student***

- Acknowledgement that core use of the device at school is for educational purposes.
- Charging, maintaining and taking care of the device.
- Appropriate digital citizenship and online safety. For more details, see ACMA CyberSmart.
- Security and password protection – passwords to be kept private and not shared with others.
- Maintaining a current back-up of files and school work, away from the device. This could be on USB storage at home, or in your OneDrive folder. Access via *www.office.com*.
- Abiding by intellectual property and copyright laws, including software and media piracy laws.
- Internet filtering when not connected to the school's network.
- Understanding and signing the BYOD Agreement.

***Parents and caregivers***

- Internet filtering, when not connected to the school's network.
- Encourage and support appropriate digital citizenship and online safety with your child.
- Some technical support. Please refer to Support and FAQ on the school website.
- Any specific software for specialist courses, including appropriate anti-virus software.
- Protective backpack or case for the device.
- Adequate warranty and insurance of the device.
- Understanding and signing the BYOD Agreement.

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

- Use mobile devices for completing classwork and assignments during class time.
- Be courteous, considerate and respectful of others when using your device.

- Switch off and/or secure the device if directed by a school staff member to enhance another aspect of learning, such as during kinaesthetic learning and practical lessons.
- Seek teacher's approval where they wish to use their device for a reason other than learning.
- Conducting themselves as positive ambassadors for the school.

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

- Using the device in an unlawful manner.
- Creating, participating in or circulating files or materials that attempt to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place.
- Disabling or hacking virus protection, spam or internet filtering.
- Downloading, distributing or publishing offensive messages or materials.
- Using obscene, inflammatory, racist, discriminatory or derogatory language.
- Using language and/or threats of violence that may amount to bullying and/or harassment
- Deliberately wasting printing and Internet resources.
- Intentionally damaging any device, accessory, peripheral, printer or network equipment.
- Commit plagiarism or violate copyright laws.
- Using unmanaged/unsupervised internet chat.
- Accessing private mobile data networks during lesson time.
- Downloading viruses or programs capable of breaching the department’s network security.
- Using the mobile device’s camera anywhere a camera would be considered inappropriate.
- Invading someone's privacy by recording personal conversations or activities and/or the further distribution of such material.
- Using the mobile device to cheat during exams or assessments.
- Take into or use mobile devices at exams or during class assessment unless permitted by staff.

**In addition to this:**

- Students must not attempt unauthorised access of other computer systems, accounts, network drives or files or 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 need to understand copying of software, information, graphics, or other data files may violate copyright laws and be subject to prosecution from agencies that enforce such laws.
- Parents and caregivers need to be aware that damage to mobile devices owned by other students or staff may result in significant consequences and costs to remedy such damage.
- 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.

**Page intentionally left blank so that the agreement page can be signed, separated from this booklet, and returned to the school.**

# BYOD Connectivity and Responsible Use Agreement

**The following is to be read and completed by both the STUDENT and PARENT/CAREGIVER. Once completed, separate from the booklet and return to the IT Support Centre (Library).**

- I have read and understood this BYOD Agreement and school rules and policies.
- I agree to abide by the guidelines contained in this and all related documents.
- I am aware that non-compliance or irresponsible behavior will result in consequences relative to the behaviour.

**Student's first name:** ...................................................................

**Student's surname:** ...................................................................…

**Current year level:** ............... **School network username (login name):** ...................................

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

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

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