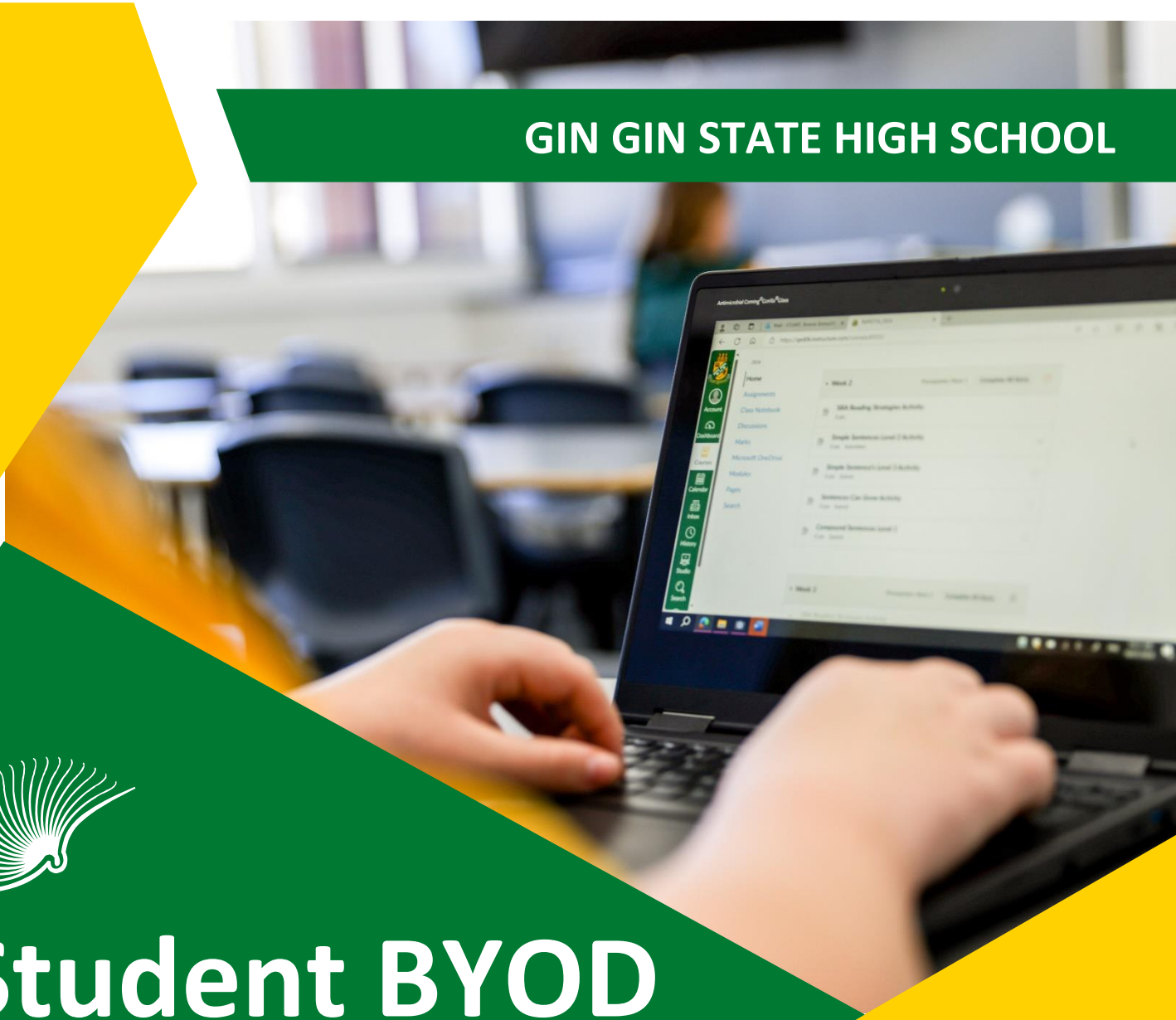
GIN GIN STATE HIGH SCHOOL



Student BYOD
Charter Agreement

BRING YOUR OWN DEVICE (BYOD) LAPTOP PROGRAM

INFORMATION FOR PARENTS/CAREGIVERS AND STUDENTS

Queensland Government

CONTENTS

STUDENT BYOD CHARTER

BYOD OVERVIEW

Bring Your Own Device (BYOD) is a new pathway supporting the delivery of 21st century learning. It is a term used to describe a digital device ownership model where students or staff use their personally-owned mobile devices to access the department's information and communication (ICT) network.

These mobile devices 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, USBs, DVDs and CDs. Access to the departments 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/user accounts.

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 the parent or caregiver and student should be aware of our school's specification of appropriate device type, operating system requirements and software. These specifications relate to the suitability of the device to enable class activities, meeting student needs and promoting safe and secure access to the department's network. Devices listed on our school portals meet the necessary requirements. Please be aware that devices purchased independently may not be able to connect.

Students are entitled to connect up to three mobile devices to the school network, **however, NO SMART PHONES are allowed on the BYOD network.**

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 schools BYOD program does not include school technical support or charging of devices at school.**

IMPORTANT NOTE: Please be aware that Windows 10 (and Prior), Windows 11 in S-Mode, Smart Phones, Android devices, Google Chromebooks, Surface RT and other devices that run Linux are NOT SUPPORTED on our BYO network.

DEVICE CARE & USAGE GUIDELINES

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.
- Keep the laptop with you at all times. Should you need to leave the laptop unattended it needs to be stored in a secure location e.g. locked classroom or IT support room.
- Consider engraving the device – engraving the bottom of the laptop with the student's name will help school staff to locate lost laptops and return them to their owners.

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. OneDrive (work or school) has been provided for students.
The backup of this data is the responsibility of the student and should be backed-up to 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.

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 Information and Communication Technologies (ICT) Student Use Agreement.

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 school's Student Code of Conduct available on the school website.

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 username 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 or staff).

- 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 set a password for access to their BYO device and keep it private.
- Students should log off at the end of each session to ensure no one else can use their account or device.

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 today 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 and caregivers are requested to ensure that their child understands this responsibility and expectation.

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 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 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. The Department of Education (DOE) operates a web filtering system to protect students and restrict access from malicious web activity and inappropriate websites.

When students are connected through DOE managed networks (including the BYO network) they will have a high level of filtering applied. This level restricts them from websites such as:

- Social networking sites e.g. Facebook, Instagram, Twitter etc.
- Open/mixed content sites e.g. YouTube
- Translation sites e.g. Google translation
- Chat sites
- Internet telephony and video conferencing sites e.g. Skype, Zoom etc.
- Document sharing and cloud storage e.g. Prezi, OneDrive, iCloud, Google Drive
- Peer to Peer sites and downloading services e.g. Bit Torrent, uTorrent, Pirate Bay, Kazzaa etc.

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.

WARNING: Outside of the DOE network, i.e. home or 4G/5G tethering to a mobile phone; is not filtered. Parent/Caregiver vigilance is a must when students are browsing the internet away from school to ensure students are not looking at inappropriate websites. Under the Gin Gin State High School BYOD program, tethering of a personal device or connecting to an unfiltered 4G or 5G connection during school times is strictly prohibited.

STUDENTS' REPORTING REQUIREMENTS

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 DOE network must also be reported to the school.

PRIVACY AND CONFIDENTIALITY

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. The student should not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. It should also be ensured 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 misuse of internet and online communication services, including accessing inappropriate sites as deemed so by the school, may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services, or involvement of the Queensland Police Service.

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.

RESPONSIBLE USE OF BYOD @ GIN GIN SHS

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 connection, care of device at school, workplace health and safety, appropriate digital citizenship and cybersafety
- Wireless connectivity to the schools BYO network via a security certificate and network password for up to three mobile devices (excluding mobile phones)
- Internet connection and Internet filtering (when connected to the school's computer network)
- Some technical support
- Printing facilities
- Access to SharePoint & OneDrive
- Some school-supplied software e.g. Microsoft Office 365

Student

- Participation in BYOD program induction
- Understanding and acceptance of the BYOD Charter Agreement.
- Acknowledgement that the core purpose of the device at school is for educational purposes
- Internet filtering (when not connected to the school's network)
- Care of the device
- Charging of the device
- Security and password protection
- Maintaining a current back-up of data
- Appropriate digital citizenship and online safety (for more details, see ACMA CyberSmart website)
- Abiding by intellectual property and copyright laws (including software/media piracy)

Parents and caregivers

- Understanding and acceptance of the BYOD Charter Agreement
- Acknowledgement that the core purpose of the 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 website)
- Some technical support e.g. home internet connection
- Any repairs required
- Required software, including sufficient anti-virus software
- Protective backpack or case for the device
- Adequate warranty and insurance of the device

IT Department at Gin Gin State High School

- Gin Gin SHS will only provide technical support to enable connectivity to the School network via the Company Portal that provides access to student files required for class, internet and printing services

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

- Using 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 and 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
- Be courteous, considerate and respectful of others when using a mobile device
- Ensure the device is fully charged before bringing it to school to enable continuity of learning
- 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 bulling 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 4G/5G networks during school 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 sharing 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.

SOFTWARE

Schools may recommend software applications 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.

Some software that Gin Gin State High School has purchased, is allowed to be installed onto students take home devices under special vendor agreements. All applications and shortcuts provided by Gin Gin State High School are for educational purposes only. The following is a list of applications and their purpose.

- **BYOx Mapper** – this application allows the device to connect to the school's printers and network drives
- **Company Portal** – this application connects the device to the BYOx-Link network
- **Microsoft Office:** Under Education Queensland's agreement with Microsoft, students can now freely access Microsoft Office 365 for Mac, Windows and iOS. Go to the website https://microsoft365.com login with the student email address and download the software

Any privately owned software installed on the device must be age appropriate, follow copyright legislation and not cause offence.

LOAN EQUIPMENT

Gin Gin State High School may provide as part of the BYOD Program, access to (for a limited period) a day-loan laptop should your student's laptop/tablet fail and require repair. The device offered is an 11.6" laptop style device that meets our schools minimum device specifications.

Conditions of Use:

- The BYOD Charter Agreement must be understood and accepted before a Day-Loan can be borrowed
- The laptop must stay at school
- The laptop must be returned to the IT support room in the Library by 3.00pm on the day it was borrowed
- The borrower and their parent/caregiver is responsible for any damage and agree to pay for any repair cost
- All policies and guidelines as per the school's Student Code of Conduct apply to the use of a Day-Loan laptop
- If the laptop is lost while borrowed, the full cost of replacement will be required
- By On-boarding your device to the Department's network you are acknowledging the above terms and conditions

Loan devices are ONLY issued when a repair ticket has been presented to the IT Department or at the discretion of the IT Department. Length of loan is no longer than 10 consecutive school days.

MINIMUM BYOD DEVICE SPECIFICATIONS

To ensure the best experience for students participating in the BYOD Program and Laptop Hire Program, we have decided on a set of minimum device specifications.

PLEASE NOTE: Surface RT, Windows 10 (and Prior), Windows 11 in S-Mode, Linux, Chromebooks and Android are NOT SUPPORTED. Devices that have less then 128GB storage are also not supported as they do not have enough available free space to install required software. Also, NO SMART PHONES are allowed on the BYO network.

MINIMUM SPECIFICATIONS	
Device type	PC Laptop, 2 in 1 Tablet PC or Mac Laptop
Processor	Intel Dual Core Pentium or higher (ARM **not currently supported**)
RAM	4GB RAM minimum
Battery Life	6 hours+
Hard Drive	128GB or above
Screen Size	11" Screen or above
Operating System	Windows 11 Mac OSX 11.7 (Big Sur) or higher **NOTE: *Windows 10 (and Prior), Windows 11 in S-Mode Android, Chromebooks, Surface RT and other devices that run Linux are NOT SUPPORTED.***
Wireless	Capable of 5ghz
Software	• Internet Browser e.g. Microsoft Edge, Google Chrome, Firefox, Safari
Features	Keyboard, USB Port, headphone port

RECOMMENDED SPECIFICATIONS	
Processor	Intel core i5 or higher (ARM **not currently supported**)
RAM	8GB or greater
Battery Life	8hrs or greater
Hard Disk	SSD (Solid State Drive) 256GB or higher
Screen Size	11" minimum
Operating System	Windows 11
Software	Office 365
Warranty	Extended to 3 or 4 years with accidental damage protection
Features	Keyboard, USB Port, headphone port, protective carry case

NOTE ON IPAD'S

iPad's have been tested and verified to work on the school's BYOD wireless network. While iPad's do not meet the minimum requirements for appropriate device type, students are permitted to connect an iPad to the school's network as a secondary device.

NOTE ON MICROSOFT FAMILY

Microsoft Family Features may not allow BYOD devices access to the School's network. Please add http://byo.eq.edu.au to the list of allowed domains.

NOTE ON WINDOWS 11 IN S-MODE

Windows 11 S-Mode is a version of Windows 11 designed for security and performance, exclusively running apps from the Microsoft Store. In order for the device to connect to the BYO Network, the device will need to be switched out of S-Mode. Instructions are available on the Microsoft support website at https://support.microsoft.com/en-us/help/4456067/windows-10-switch-out-of-s-mode.

VENDOR PORTALS

As a service we provide parents with access to laptop portals to assist in the purchase of suitable, quality devices at the best price. The vendor portals include a variety of brands and a range of price points.

The portal laptops have been carefully selected to meet the following criteria:

- **Durability** – devices built for education with strength and reliable battery life (these are not available in retail stores)
- **Warranty and Accidental Damage Protection (recommended)** warranty and insurances that are not available to the retail market.
- **Compatibility –** operating systems that are compatible with the school's managed network
- **Price** – educational pricing, payment plans and interest free options.

Please note, the school does not endorse any one supplier, parents/guardians can choose to purchase from where ever they desire (online or in-store). To purchase via one of the vendor portals, please click on the links below or navigate to the website URL.

The School Locker (Harvey Norman)
theschoollocker.com.au/catalog/category/view/s/technology/id/14784/

HP Vendor Portal
www.hp.com/au-en/shop/byod/gingin

Dell Vendor Portal. Username: ginginshs **Password:** parent
datashop-qld.datacom.com.au/ginginshs

Apple Education Portal
apple.com/au-hed/shop

SCHOOL CONTACTS

Below are the contact details for the IT Department at Gin Gin State High School. If you have any questions or require any further information regarding the Student BYOD program, please do not hesitate to contact us.

Email: byox@ginginshs.eq.edu.au
Phone: (07) 4133 2111

The IT Support Room is open for students to access at the below times:

	Monday	Tuesday	Wednesday	Thursday	Friday
Before School	8:15 – 8:45	8:15 – 8:45	8:15 – 8:45	8:15 – 8:45	8:15 – 8:45
First Recess	11:15 – 11:55	11:15 – 11:55	11:15 – 11:55	11:15 – 11:55	11:15 – 11:55
Second Recess	1:05 – 1:35	1:05 – 1:35	1:05 – 1:35	1:05 – 1:35	1:05 – 1:35
After School	2:45 – 3:00	2:45 – 3:00	2:45 – 3:00	2:45 – 3:00	2:45 – 3:00