BYOD
BRING YOUR OWN DEVICE

Information Guide & User Agreement
for parents and students

FLAGSTONE

State Community College

Contents

What is BYOD?

Bring Your Own Device (BYOD) is a term used to describe a digital device ownership model where students use their personally-owned mobile devices to access departmental networks and information management systems in an educational setting. Flagstone State Community College understands that it is a tool that enhances pedagogy, facilitates the creation and sharing of knowledge, and allows differentiation in learning. The use of technology is more than a method of retrieving information.

The use of a laptop:

- Enhances independence and self-initiated learning among students.
- Allows teachers to expand our instructional strategies and personalise learning for students.
- Extends student learning beyond the classroom.
- Promotes the development of 21st Century teaching and learning. Modern teaching practices requires the use of a digital platform (e.g. OneNote).
- Provides skills and experiences that will prepare them for their future studies and careers.
- Allows for effective engagement. Our Gen Z students are visual, adaptive, flexible and collaborative learners.
- Assists students to become responsible digital citizens.

BYOD Rollout - Teaching and Learning

In 2022, all Year 7-12 students will be part of the BYOD program. Teaching and learning will continue to transform with increased access to devices by students. How this is achieved will be different in each year level and subject area. Through use of digital content, concepts can be taught faster and with a higher level of individualisation, and students can be more productive in learning time.

Each student will have access to eLearning spaces (e.g. Class Notebook) to access teaching and learning resources. These spaces will be set up by their teachers.

NOTE: At school the laptop will be used for education purposes, NOT a recreational purpose. The student's use of their device, in and out of class, is determined by a teacher. At all times the student is obliged to follow a teacher's instructions regarding the use of the device.

Device selection

To enable connection to our network, it is important the device meets the **minimum specifications (left column)** outlined below. This will ensure the device is able to connect to the school network, printing systems, and suitable for class activities.

If financial circumstances allow, the **recommended specifications (right column)** will benefit students greater through increased speed and capabilities. This will lead to less frustration from students!

NOTE: Please DO NOT buy a Chromebook…they do not work on the Education Queensland network!

	Minimum Specifications (Good)	Recommended Specifications (Better)
Platform	Windows PC or Apple Macintosh	
Screen Size	11”-14” display – consider portability and weight	12”-14” display – consider portability and weight
Processor	Intel Core i3/Dual Core processor	Intel Core i5/Quad Core processor or higher
RAM	4 GB	8 GB or higher
Hard Drive	128 GB Solid State Hard Drive (note: we recommend a solid state hard drive (SSD) for reliability, durability and speed) Older style Hard Drives are not as reliable, however, if this is your only option, min 250 GB would be best.	256 GB Solid State Hard Drive (note: we recommend a solid state hard drive (SSD) for reliability, durability and speed)
Operating System	Microsoft Windows 10 (minimum) Note: The version of Windows called “Windows 10S” is **NOT** compatible. **NOT Supported: Android, Windows RT, Chromebook and distributions of Linux**	
Wireless	Wi-Fi 802.11ac/n or better (Wireless Network 5Ghz). The above specs are a ‘must have’ otherwise the device will not connect to our network.	
Battery	Sufficient to last 6+ hours on balance power mode	
Features	USB ports, headphone port, in-built microphone, webcam	

In regards to laptops…

Students will like:

- light weight
- wireless mouse
- headphones

Parents will like:

- Protective hard case to reduce the instance of a broken screen (don't be tempted to buy a soft laptop sleeve).
- Onsite warranty (next business day is recommended – having to send a PC away for a couple of weeks for a warranty repair can be frustrating).
- Accidental damage protection / insurance – may be offered at time of purchase.
- Back-up storage device (USB or External Hard Drive) to back up files on the laptop.

Purchasing Considerations

It is recommended that parents/caregivers contact a range of computer vendors and consider the 'total cost of ownership' including warranty, technical support arrangements and hardware components which will contribute to the life of the laptop. The cheapest laptop to buy is generally not the best option in the long run.

As a starting point, links to a number of vendor website portals/online stores are available for parents/guardians on our College website. Parents/guardians can purchase a device through these portals or take the minimum specifications into a local computer supplier. Another purchasing option to consider are ex-government refurbished laptops.

The College takes **no** responsibility for any private laptop purchasing and/or finance arrangements. All issues with laptop purchases or technical issues must be taken up with the vendor/supplier.

What if I can't afford a laptop?

Families experiencing financial hardship can apply for an equity device. To be considered for an equity device, students must be a financial member of the College Shared Resources Scheme. More information about the Equity Policy and an online application form, can be found on our college website - https://flagstonescc.eq.edu.au/curriculum/bring-your-own-device/4-b-y-o-d-equity-policy.

A limited number of older laptops are available for daily borrowing (9am-3pm) from ST13 for students who arrive to school without a laptop.

Software Requirements

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.

Software installation is the responsibility of the student/parent/caregiver. Valid licences are required for all software present on the device. It is recommended that every device has the following software installed.

Minimum Software Requirements

Microsoft Office	'Microsoft Office Advantage' allows students to install the Office suite of software (e.g. Word, Excel, PowerPoint etc) for FREE. Instructions to download, install and activate this software are available from https://learningplace.education.qld.gov.au/microsoft-office-software
Virus Protection	Parents can install their usual anti-virus software on the laptop. Windows 10 also has built-in real-time antivirus named *Windows Defender*. *Defender* is sufficient to pass the virus software check.

Other Suggested Software

Internet Browsers	
Google Chrome	http://www.google.com/chrome
Adobe Creative Cloud	
As Flagstone SCC subscribes to the Adobe Software Agreement, this software is available for students to purchase at a reduced rate.	Please speak to the IT technicians in ST13 if you would like to purchase Adobe Creative Cloud. Students will be invoiced $10 for the cost of the program. Access to Adobe CC expires at the end of the year that the product was purchased. Recommended to only be installed on those laptops that meet the "recommended specifications" listed on page 4.
Video Players	
VLC Player	http://www.videolan.org/vlc
Audio Recorder	
Audacity	https://www.audacityteam.org/download/
Plugins	
Adobe Acrobat Reader DC	https://get.adobe.com/reader/

Laptop Connectivity

Student private laptops connect to the College network through the Department of Education technical service called BYOxLink. BYOxLink service allows students to securely access the IT network, printers, school email and mobile learning applications on their own devices. It provides seamless access to digital learning resources between school and home.

The department has selected Microsoft Intune as its mobile device management (MDM) tool. One-to-one devices in schools that use BYOxLink need to enrol into the Microsoft Intune Company Portal (Intune). Intune allows the department to distribute a wireless network profile and curriculum related applications to student's BYO devices.

School staff can only access school information through Intune and cannot:

- see personal information
- monitor what happens on the device
- track or locate the device
- see information on installed personal applications (other than school applications)
- uninstall applications, including personal ones.

More information about BYOxLink and installation guides can be found at https://flagstonescc.eq.edu.au/curriculum/bring-your-own-device/7-preparing-your-device-for-school

Laptop Charging

It is the responsibility of the student to bring their laptop to school fully charged every day. Failure to bring laptops fully charged each day will impact on student learning and their ability to participate in class activities. Students will NOT be able to charge laptops in classrooms or the library. This is primarily due to workplace health and safety issues (e.g. cables being a trip hazard, power cables not “tested and tagged”). However, if a student requires their laptop to be charged (e.g. if it’s an older laptop that doesn’t hold its charge) there will be a charging station in ST13 (Technicians Room) that students will be able to access before school and at break times to charge their laptops securely. Students will need to bring their charging cables to school to successfully utilise this facility.

Technical Support

College IT Technicians will provide support for connectivity of laptops to the College network. Every attempt will be made to connect devices which meet the minimum specifications, assuming there are no technical or other issues outside their control. All other technical issues will be the responsibility of the parent/caregiver and student. Vendor and technical support turnaround times should be considered when purchasing and seeking repairs for devices.

	Internet Connection	Hardware	Software
Students, Parents & Caregivers	✓ (home-provided internet connection)	✓	✓
School	✓ (school provided internet connection)	×	✓ (some school-based software arrangements e.g. Office, Adobe)
Device Vendor	×	✓ (see specifics of warranty on purchase)	×

Device care

Students bring their own device for use at Flagstone State Community College at their own risk. The College **will not** be responsible for any loss, theft or damage to the device or data stored on the device. In circumstances where a device is damaged by abuse or malicious act of another student, the school will apply consequences in accordance with the Student Code of Conduct. However, we are not liable for the reimbursement or replacement of the device.

Parents and students should consider whether their device requires insurance and whether specific accidental loss and breakage insurance is appropriate for the device. 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.

Suggestions to keep the laptop secure at school:

- Keep the laptop with you at all times. Do NOT leave it in your bag outside of classrooms.
- Short term storage in a locker – lockers have been provided in the Science & Technology building for any student to use for the TEMPORARY storage of their laptops (e.g. safe-keeping during a practical lesson or at lunchtimes). Students can safely secure their laptop for the duration of the practical lesson and remove it at the end. NOTE: locks left on a locker at the end of the day may be removed.
- Consider engraving the device – this will help identify any lost devices.

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 carry the device by the screen – carry it holding the base of the laptop.
- 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.

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. 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.

Students also have access to Microsoft OneDrive, a cloud-based storage, allowing students access to their documents on any Internet enabled device.

Acceptable personal 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 Department of Education’s procedure – Use of ICT systems.

This procedure also forms part of this BYOD Responsible Use Agreement. The acceptable-use conditions apply to the use of the device and internet both on and off the school grounds.

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 BYOx 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.

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 Student Code of Conduct and any specific rules of the school. To help protect students (and staff) from malicious web activity and inappropriate websites, the school operates a comprehensive web filtering system. Any device connected to the internet through the school network will have filtering applied.

The filtering system provides a layer of protection to staff and students against:

- inappropriate web pages
- spyware and malware
- peer-to-peer sessions

- scams and identity theft.

This purpose-built web filtering solution takes a precautionary approach to blocking websites including those that do not disclose information about their purpose and content. The school's filtering approach represents global best-practice in internet protection measures. However, despite internal departmental controls to manage content on the internet, illegal, dangerous or offensive information may be accessed or accidentally displayed. Teachers will always exercise their duty of care, but avoiding or reducing access to harmful information also requires responsible use by the student.

Students are required to report any internet site accessed that is considered inappropriate. Any suspected security breach involving students, users from other schools, or from outside the Queensland DET network must also be reported to the school.

The personally-owned devices have access to home and other out of school internet services and those services may not include any internet filtering. Parents 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.

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.

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.

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 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.

STYMIE

We are a STYMIE School. The word "STYMIE" means to stop or thwart. We want bullying to stop and so do our students.

STYMIE is an on-line anonymous notification system that students can use to report bullying or harm. STYMIE is a web application, meaning that students can access it via any internet browser. They do not have to download anything from a website or store. Students can use any internet-connected device to make a notification at any time.

STYMIE allows students to support their peers in cases of overt and covert bullying. STYMIE empowers bystanders with the confidence to stand up for each other without fear; we are teaching them to say something. By enabling our students to report incidents of bullying and harm, safely and anonymously, STYMIE equips our students with the tools to be an up stander, rather than a bystander – an up stander is someone who supports their peers in times of need.

The web-app prompts students to write a short description of an incident involving bullying or harm. They can also upload supportive evidence using screenshots of aggressive, threatening or harassing social media content or messages. The school will receive notifications via email and will deal with them according to our Responsible Behaviour Plan and Positive Relationships, Safe Schools Policy.

https://stymie.com.au

Intellectual property and copyright

Students should never plagiarise information and should observe appropriate copyright clearance, including acknowledging the original author or source of any files, information, images, audio 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.

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.

Standard school behavior management procedures apply for misuse of any BYOD item. While at school, all material on the devices is subject to review by school staff. Students are to connect their device to the designated wireless network only. Students are not to create, participate in, or circulate content that attempts to undermine, hack into and/or bypass the hardware and software mechanisms that are in place.

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 and printing connection at school (to print, students must be a current Student Resource Scheme member)
- internet filtering (when connected via the school's computer network)
- some technical support (please consult Technical Support section of this booklet)
- some school-supplied software e.g. Microsoft Office 365
- printing facilities (to print, students must up-to-date in the Student Resource Scheme).

Student

- participation in BYOD program induction
- acknowledgement that core purpose of device at school is for educational purposes
- Ensure that personal use if kept to a minimum and internet and online communication services are generally used for genuine curriculum and educational actives. Use of unauthorized programs and intentionally downloading unauthorized software, graphics or music that is not associated with learning, is not permitted.
- care of device
- appropriate digital citizenship and online safety
- 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)
- technical support (please consult Technical Support section of this booklet)
- 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 BYOx 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
- technical support (please consult Technical Support section of this booklet)
- 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 User Agreement.

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 Student Code of Conduct.
- 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.

Flagstone SCC BYOD User Agreement

The Flagstone State Community College BYOD Program gives freedom to students and their families to tailor their choice of technology to their own educational needs. However, students and parents must be aware of and consent to the program's boundaries described in this agreement.

Equipment

The devices must be brought to school by the student every day and will be solely theirs to use. The device must meet the minimum specification requirements as outlined in the Parent Information Book.

Responsible use agreement

The Flagstone State Community College BYOD Program aims to improve students learning experiences both in and out of the classroom. The school does so with the expectation that students will make good decisions with regard to their personal use of technology.

The BYOD Responsible Use Agreement must be agreed to and signed before student are permitted to bring their device to school and connect to our network. Students and parents/carers must carefully read the information contained in this booklet prior to signing this agreement. Any questions should be addressed to the College and clarification obtained before the agreement is signed.

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

- I have read and understood the BYOD Information Booklet, BYOD User Agreement and Student Code of Conduct (available on the school website).
- We understand our responsibilities regarding the use of the device at school and the connection to the school network and internet, as outlined in the documents.
- In signing below, we understand and agree to the information contained in the BYOD Information Booklet and BYOD User Agreement.
- We understand that failure to comply with the BYOD Information Booklet and BYOD Agreement will invoke the school's standard discipline procedures, which includes, but is not limited to, the withdrawal of access to school supplied services.
- When at school, the student's use of their device, in and out of class, is determined by a teacher and will be used for an educational purpose. At all times the student is obliged to follow a teacher's instructions regarding the use of the device.
- Students bring their own device for use at Flagstone State Community College at their own risk. The College will not be responsible for any loss, theft or damage to the device or stored data.
- This agreement lasts for the duration of enrolment at Flagstone State Community College.

Student's name: ..... **Year:** .....

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

Parent's/caregiver's name:.....

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

Flagstone SCC BYOD Equity Policy

Rationale

The Flagstone State Community College BYOD program imposes a financial cost on students and their families in supplying a device. At the same time, the program can only function if all students have access to appropriate technological resources in all their classes. Flagstone SCC takes seriously the role of public education in ensuring all students have access to the same learning outcomes. The purpose of the BYOD Equity Policy is to establish the framework for the BYOD program to provide this for all students, irrespective of their families' financial means.

Actions

Flagstone State Community College will:

1. Ensure the BYOD Program's Minimum Device Specification is designed so that a range of devices in varying capability and cost are offered and meet the minimum specification.
2. Assess applications for assistance on a case-by-case basis.

Due consideration will be given to all the facts of the matter, including:

- The level of assistance requested.
- If the student is part of the shared resource scheme.
- The year level of the student.
- The subjects the student undertakes
- The technology already available to the student at school and at home.

Students and Parents/Carers:

1. Consider options for the purchase of equipment that meets the minimum device specifications.
2. If you believe you are unable to provide a device that meets the minimum specifications:
    a. The school will liaise with you, your student and their teachers to identify the most appropriate way to address the issue.
    b. You will be asked to make an agreement with the school that confirms the alternative arrangements made for your student's access to technological resources.
3. The College has limited devices it can provide for short term loan. On approval by the Principal, a device will be loaned to your students for the negotiated period of time.

To apply for an equity device, please visit our college website and complete the online BYOD Equity Application Form - https://flagstonescc.eq.edu.au/curriculum/bring-your-own-device/4-b-y-o-d-equity-policy