# BROOKSIDE P-9 COLLEGE



# BRING YOUR OWN DEVICE (BYOD) PROGRAM 7-9

# PARENT INFORMATION BOOKLET

## BROOKSIDE COLLEGE: FUTURE READY LEARNERS

At Brookside College we are committed to helping every learner develop as a whole person, fulfil his or her potential and help shape a shared future built on the well-being of individuals, communities and the planet.

At Brookside College we believe education has a vital role to play in developing the knowledge, skills, attitudes and values that enable people to contribute to and benefit from an inclusive and sustainable future. This includes learning to form clear and purposeful goals, work with others with different perspectives, find untapped opportunities and identify multiple solutions to big problems.

At Brookside College we use digital technologies to ensure our learners are future ready. In 2019, Year 7 students and new Year 8 & 9 students will have the opportunity to participate in a BYOD (Bring Your Own Device) Program. Students will need to demonstrate commitment to being a responsible learner. This means meeting attendance and punctuality standards and using the device in strict accordance with the College's ICT Acceptable Use Policy. The Laptop program provides an opportunity for our students to enter a new world of curriculum possibilities, allowing engagement and involvement in their learning.

## BRING YOUR OWN DEVICE (BYOD)

The BYOD program allows students to bring their own device from home or purchase from a retailer. ***The College does not manage the device in any way***, including loss, damage and accidents. Students will be required to bring the device to the ICT office for configuration of school resources and to provide access to the school network. They will be given access to the college Wi-Fi, printing and DET software, such as Microsoft Office through an online "software centre" (the link and instructions for students to download and install their copy licenced by DET will be provided by the ICT technicians at this time). The student is required to run all Windows/MAC updates.

*\*\*Please note: It is recommended that students participate in the BYOD Program and those students who do not participate in the BYOD Program will have very limited access to school owned laptops.*

In order to support families in making the decision about an appropriate device, parents are advised to check the following recommendations before making a BYOD purchase:

DEVICE MINIMUM SPECIFICATIONS

| MICROSOFT WINDOWS | APPLE - MACBOOK |
|---|---|
| <ul><li>4GB or higher RAM (memory)</li><li>128GB or higher hard drive storage</li><li>Windows 10 or higher</li><li>Battery Life +6 hours</li></ul> | <ul><li>4GB or higher RAM (memory)</li><li>128GB or higher hard drive storage</li><li>Mac OS X v10.12 or higher</li><li>Battery Life +6 hours</li></ul> |
| APPLE iPad | |
| <ul><li>Generation 6 or higher</li><li>Battery Life +6 hours</li><li>Keyboard Recommended</li></ul> | |

**In alignment with the Brookside College Mobile Phone Policy, students cannot use a mobile phone during school hours and a mobile phone cannot be used as part of the BYOD Program.**

**Tips for looking after your device:**

- Always close your device when carrying it, to prevent screen damage.
- Always use a carry bag as they are designed to reduce the impact of drops.
- Don't drink anywhere near your device (this includes family members).
- Think twice before shutting the screen – is there anything on the keyboard?
- Always ensure cables are well out of the way to avoid tripping over them.
- Have your device fully charged before bringing it to school.
- Never leave your device in an unlocked car.
- Never leave your device unattended in public, even for a short time.
- Never pick up your device by its screen.
- Don't wrap the cord too tightly around the power adaptor because this might damage the cord.
- Gently brush your keyboard with a clean soft bristled paint brush or similar to remove dirt.
- When unplugging the power cord, pull on the plug itself rather than the cord.
- Lightly dampen a non-abrasive cloth with water and gently wipe screen in a circular motion. Do not directly apply water or cleaner to the screen.

**Cyber-bullying or inappropriate use**

The device must not be used in any way to send messages, take photos or take part in any form of cyber-bullying. Students are expected to be aware of their social activities online. The College will support this by teaching students about appropriate online behaviour. If they are caught using the device for cyber-bullying or inappropriate behaviour, follow up action will result in time without the device and notification to parents.

**What if the device is damaged, lost or stolen?**

Parents are strongly encouraged to purchase insurance to cover for accidental damage, loss and theft of the device. Quite often house and contents insurance provides coverage for this and is worth investigating prior to completing your device purchase.

**Software Licensing**

Software installed by the school is subject to licence conditions and must not be distributed or deleted without written permission from the school.

**Internet Usage**

Student device use is governed by the "Acceptable Use Agreement" that students and parents agree to prior to use of ICT within the college. Familiarisation with this policy will also further support the student's adherence outside of the school environment. Any inappropriate use of the internet is unacceptable and is subject to disciplinary action and exclusion from the school networks and resources.

Appropriate use of the internet service within the school network is closely monitored by a filtering system which allows for inappropriate content blocking by a regularly updated list of categories and sites. This does not apply to use of devices outside of the school network. Education and support are important for maintaining acceptable use of devices, particularly in relation to internet access.

**Viruses**

Viruses have the potential to severely damage and disrupt operations within the school and DET's computer networks. As students have the right to add software on their devices and connect to the internet from home, they should take all steps to protect the school and DET's computer network from virus attacks.

The device must have current up to date antivirus software installed on them. This software will scan the hard drive for known viruses on start-up. The virus software will be upgraded from the network.

Students are recommended to:

- Consider running virus scans regularly after accessing the internet or personal mail or opening a file from a removable media source. Carry out the scan before returning to the school and connecting to the school network.
- Not to open any files attached to suspicious or unknown emails.
- Exercise caution when downloading files from the internet. Save the files to the device hard disk and run the virus scanner on the file before opening them.
- Delete chain and junk emails. Do not forward or reply to any of these.
- Never reply to spam. Spam email messages can contain viruses that notify a third party of the legitimacy of an email address and then add the recipients to the spammer's database. They can also consume a large amount of disk space on the server, which slows computer networks.
- Shutdown/restart computer on a weekly basis in order to keep Windows/MAC updates current.

**Non-school Applications and Files**

Software, including music, movies and games will be allowed for academic and recreational reasons, provided copyright obligations are met. No games, music, movies or other material that contain obscene language, offensive content or are rated higher than PG are permitted to be accessed whilst on College grounds. Downloading music, games and videos from the internet during school hours is prohibited except when directed by a staff member. Students are permitted to listen to digital music and/or participate in games on their device while at School when given express permission by a teacher for an educational purpose. It is the student's responsibility to ensure that there is enough hard drive space and memory available to engage in all educational requirements.

**Power Supply Management**

Devices are to be fully charged at the commencement of every day. Please charge your device according to the manufacturer's guidelines to get the most out of your battery. There will be no availability to charge any devices at the College.

**Backup and Recovery**

Students will be responsible for their own backup of critical data at all times. This may be through a USB, external drive, or on their individual home drive on the College server to regularly backup important work. No video games, movies or music is to be stored or saved on the school server. Students are responsible for backing up any software, programs, music or work they load or create on their device.

**Padlock**

All students are required to purchase a lock for their locker before bringing their device to school for the first time.

**Here is a go-to list of things students can and cannot do on laptop whilst on College grounds.**

**You CAN....**

- Download any programs, apps or games that are offered on the Windows/MAC App Store (paid or free). *Any programs, apps or games that are rated higher than G or PG **must not** be viewed or shared whilst on College grounds.*
- Purchase music or games (rated G or PG) legally. *Anything rated higher than G or PG **must not** be viewed, listened to or shared whilst on College grounds.*
- Use the camera or microphone when instructed by a teacher.
- Use the laptop in the library during lunchtimes.
- Browse the web (including social media websites) at home, *HOWEVER BEWARE: everything you search and look at is recorded and can be recovered by the school's IT Technician.*
- Label the laptop (engraving your name would be ideal).

**You CANNOT...**

- Use the laptop to illegally download content such as movies, music, games and programs (e.g. torrent programs).
- Use VPN or Proxy bypass software at school.
- Play or download any content (music, movies, games, etc.) that is rated higher than PG whilst on College grounds.
- Use the camera or microphone at school unless given permission by a teacher.
- Have any inappropriate or offensive images set as desktop wallpaper.
- Use the laptop in the school yard during lunch and recess.
- Bring the charger to school (this is an OHS requirement).
- Use Skype whilst on College grounds.
- Use social media apps or websites while at school.
- Graffiti your laptop/tablet.
- Lend/swap/borrow laptops or laptop parts (i.e. detachable screens and keyboards) with other students.

**If you are unsure of anything, <u>ask a teacher</u> or the <u>Year Leader</u>. Use the laptop appropriately and you will be able to enjoy all the benefits it provides!**

# *Advice for Parents*

The College believes the teaching of cyber-safe and ethical online behaviour is essential in the lives of students and is best taught in partnership between home and school. 21st Century students spend increasing amounts of time online learning and socialising. These online communities need cybercitizens who do the right thing by themselves and others online, particularly when no one is watching. Safe and ethical behaviour online is explicitly taught at our school and support at home is requested. It is important to note that some online activities are illegal and as such will be reported to police. This includes harassment of others and the publishing of inappropriate images.

### *Bridging the gap between home and school*

At school the internet is used to support teaching and learning. At home, however, it is often used differently. Not only is it a study resource for students, but it is increasingly being used as a social space to meet and chat.

If you have the internet at home, encourage your child to show you what they are doing online.

At home we recommend you:
- Find out how your child uses the internet and who else is involved in their online activities.
- Have the computer with internet access in a shared place in the house – not your child's bedroom.
- Ask questions when your child shows you what they are doing, such as:
    - How does it work and how do you set it up?
    - Who else is sharing this space or game?
    - Can you see any risks or dangers in the activity?
    - What are you doing to protect yourself or your friends from these potential dangers?
    - When would you inform an adult about an incident that has happened online that concerns you?

Statistics show that students will not approach an adult for help because:
- they might get the blame for any incident.
- they don't think adults "get" their online stuff.
- they might put at risk their own access to technology by either admitting to a mistake or highlighting a situation that might lead a parent to ban their access.