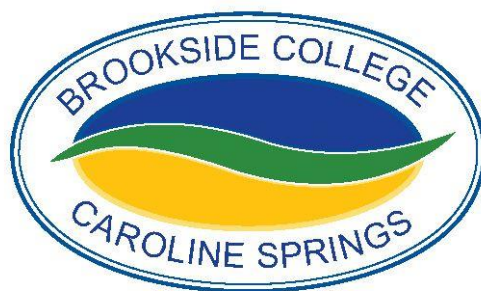


Brookside P-9 College Device Program 2018

Parent Information Booklet



Learning experiences across the school are purposefully designed to develop the attributes of a life-long learner. In this way, each student learns to develop and demonstrate the knowledge, skills, practices and attitudes necessary to be an engaged, robust, 21st century citizen capable of shaping our future. In 2018, Year 7 students and new Year 8 & 9 students will have the opportunity to participate in a SMD (School Managed Device) or 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.

Option 1 – School Managed Device (SMD)

The School Managed Device program helps to provide a more standardized approach to the implementation of technology within the College and is Brookside P-9 College's preferred option. Apart from parents arranging purchase and payment arrangements with either of our designated suppliers (Learning with Technologies or JB Hi-Fi), all other aspects of this program will be organised and maintained by the school.

Brookside P-9 College have selected the Lenovo 11e Thinkpad as its mainstay machine, with three device options provided to cater for those Parents opting to purchase a device with higher specifications. The chosen devices provide a balance of performance, reliability and service whilst providing parents with options in regards to cost.

These devices are bought directly from either Learning with Technologies (LWT) (<http://brooksidep9.orderportal.com.au/>) or JB Hi-Fi (<https://www.jbeducation.com.au/byod/> school code: **brooksidebyod**) via an online portal specifically for Brookside P-9 College. The device can be purchased outright, paid by instalments using BPAY (JB Hi-Fi only) or by entering into interest free arrangements. Parents can also, of course, make their own private finance arrangements and purchase the device from either of the suppliers via the portal. **If choosing this option, please ensure you read the information on the portals regarding delivery dates and order cut off dates.**

Payment for the device and warranty are compulsory, with the case and insurance optional. Parents are encouraged to check whether their house and contents insurance provides coverage for accidental damage, loss and theft. If not, it is highly recommended that parents purchase this insurance at the same time as purchasing the device.

Once purchased, warranty claims and technical support such as imaging and updating security will be supported by the technicians at Brookside P-9 College. These devices will have the full Edustar suite of software as specified by DET at the time. Parents will be required to lodge and manage insurance claims independently from the College (if insurance cover is purchased).

Option 2 – Bring Your Own Device (BYOD)

The BYOD program allows students to bring their own device from home or purchase from a retailer other than via the designated portals under Option 1. The College does not manage the device in any way. 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 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 ensure the device has anti-virus and security software installed at all times.

If electing to participate in Option 2, it must be made clear that students will not have access to our school technicians for repairs, breakages, software issues (other than software licenced to DET), updates and downloads. Parents will be required to organise any repairs, warranties or insurance issues themselves.

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 style="list-style-type: none">• 4GB or higher RAM (memory)• 64GB or higher hard drive storage• Windows 8 or higher• Battery Life +6 hours	<ul style="list-style-type: none">• 4GB or higher RAM (memory)• 64GB or higher hard drive storage• Mac OS X v10.9 or higher• Battery Life +6 hours

Please note, IPADS or devices running on android, chrome or IOS operating systems are not suitable and can not be supported.

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. If purchasing through either of the portals (LWT or JB Hi-Fi) please be advised that insurance can only be purchased at the same time as purchasing the device. There will not be the option to go back and add on insurance once the transaction has been completed.

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.

Students who elect to purchase a device through JB Hi Fi or LWT (Option 1-School Managed Device) will have the full Edustar image provided on the device. Students who are bringing their own device (Option 2 – Bring Your Own Device) will have access to some of the DET programs (eg. Microsoft office).

Internet Usage

Student device use is governed by the “Acceptable Use – Middle Years Policy” 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:

- Protect their devices from virus attacks by scanning for viruses at least weekly. Microsoft virus definitions updates are managed automatically by the school network.
- 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.

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 where 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.

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 share 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. When a device needs to be reimaged, the initial DET image will be installed back onto the devices purchased via JB Hifi or LWT. Students are responsible for backing up any software, programs, music or work they load or create on their device.

School Padlock

All students are required to purchase a lock for their locker before bringing their device to school for the first time. Students can provide their own or the office has a limited supply of padlocks that can be purchased at a

cost of \$25. Please note that padlocks purchased from the College can be unlocked with a masterkey by your child's Year Leader should they leave their key at home. If you feel that there is a possibility of this happening to your child, you may wish to purchase the lock from the College.

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

You CANNOT...

- Use the laptop to illegally download content such as movies, music, games and programs (e.g. torrent programs).
- 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.
- Place stickers on or graffiti your laptop/tablet.
- Lend/swap/borrow laptops or laptop parts (i.e. detachable screens and keyboards) with other students.

You CAN...

- Download any programs, apps or games that are offered on the Windows 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).

If you are unsure of anything, ask a teacher or the Year Leader. 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 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 any 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 is 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

How is Technology Used to Bully?

Technology can be used both positively and negatively. The table below explores the range of ways today's technology can be used.

Technology:	Great for:	Examples of misuse:
 <p>Mobile phones</p>	Keeping in touch by voice or text, taking and sending pictures and film, listening to music, playing games, Going online and sending emails. Useful in emergency situations and for allowing children a greater sense of independence.	Sending nasty calls or text messages, including threats, Intimidation, harassment. Taking and sharing humiliating images. Videoing other people being harassed and sending these to other phones or internet sites.
 <p>Instant Messenger (IM)</p>	Text or voice chatting live with friends online. A quick and effective way of keeping in touch even while working on other things.	Sending nasty messages or content. Using someone else's account to forward rude or mean messages via their contacts list.
 <p>Chatrooms and Message boards</p>	Groups of people around the world can text or voice chat live about common interest. For young people, this can be an easy way to meet new people and explore issues which they are too shy to talk about in person.	Sending nasty or threatening anonymous messages. Groups of people deciding to pick on or ignore individuals. Making friends under false pretences- people pretending to be someone they're not in order to get personal information that they can misuse in a range of ways - e.g. by spreading secrets or blackmailing.
 <p>Email</p>	Sending electronic letters, pictures and other files quickly And cheaply anywhere n the world.	Sending nasty or threatening messages. Forwarding unsuitable content including images and video clips, or sending computer viruses. Accessing someone else's account, e.g. to forward personal emails or delete emails.
 <p>Webcams</p>	Taking pictures or recording messages. Being able to see and talk to someone live on your computer screen. Bringing far-off places to life or video conferencing.	Making and sending inappropriate content. Persuading or threatening young people to act in inappropriate ways. Using inappropriate recordings to manipulate young people.
 <p>Social network sites</p>	Socialising with your friends and making new ones within online communities. Allowing young people to be creative online, even publishing online music. Personalising homepages and profiles, creating and uploading content.	Posting nasty comments, humiliating images/video. Accessing another person's account details and sending unpleasant messages, deleting information or making private information public. Groups of people picking on individuals by excluding them. Creating fake profiles to pretend to be someone else, e.g. to bully, harass or get the person into trouble.
 <p>Video hosting sites</p>	Accessing useful educational, entertaining and original creative video content and uploading your own.	Posting nasty comments, humiliating film of someone.
 <p>Virtual Learning Environments (VLEs)</p>	School site, usually available from home and school, set Up for tracking and recording student assignments, tests and activities, with message boards, chat and IM.	Posting inappropriate messages or images. Hacking into someone else's account to post inappropriate comments or delete schoolwork.
 <p>Gaming sites, Consoles and Virtual worlds</p>	Live text or voice chat during online gaming between players across the world, or on handheld consoles with people in the same local area. Virtual worlds let users design their own avatars - figure that represents them in the virtual world.	Name-calling, making abusive / derogatory remarks. Players may pick on weaker or less experienced users, repeatedly killing their characters. Forwarding unwanted messages to other devised in the immediate vicinity.