'Balit Yirramboi'

Dohertys Creek P-9 College

TRUGANINA

BYOD Program

Parent Information Booklet

(Years 3-9)

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, global citizen capable of shaping our future. At Dohertys Creek P-9 College, our **Grade 3-9 students** will have the opportunity to participate in a **BYOD (Bring your own device) *laptop* 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 Digital Learning 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 - Purchase via the Learning with Technologies (LWT) Portal

This option helps to provide a more standardized approach to the implementation of technology within the College.

Dohertys Creek P-9 College have selected the Lenovo 500w Gen 3 as their 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 purchased directly from Learning with Technologies (LWT) (https://dohertyscreekcollege.orderportal.com.au/) via an online portal specifically for Dohertys Creek P-9 College. The device can be purchased outright, paid for by instalments using BPAY or by entering into interest free arrangements. **If choosing this option, please ensure you read the information on the portal regarding delivery dates and order cut off dates**.

Payment for the device and warranty are compulsory, with an extended battery warranty 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, the device will be delivered to your home. Delivery is estimated to be mid December (if ordered by the cut off date). At the beginning of the new school year, our technicians and teachers will guided students in how to download DET licenced software and connect to our network.

Parents will be required to lodge and manage repairs, warranty & insurance claims independently from the College (if insurance cover is purchased) however an LWT technician will attend onsite to complete warranty repairs where possible.

Option 2 – Bring Your Own Device from home

Dohertys Creek P-9 College also allows students to bring their own laptop device from home or purchase from a retailer other than via the designated portal in Option 1. During the first week of the new year, students will be guided by our school IT technicians and teachers to access the school network and download DET licensed software. This includes 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 the operating system is not Windows 10.

Parents will be required to manage repairs, warranty & insurance claims independently from the College.

Please note: It is highly recommended that students participate in the BYOD Program to enhance their learning opportunities. Students who do not participate in the BYOD Program will have limited access to school owned laptops.

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:

- Intel Core I3 Generation 3 or higher
- 8 Gb ram
- 128 Gb Hard drive SSD
- WiFi – must support 2.4Ghz wireless and preferably 5Ghz 802.11 Abgn WiFi
- Webcam
- USB ports x 2
- Support windows 10

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

In alignment with the Dohertys Creek P-9 College mobile phone policy, students cannot use mobile phones 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. If purchasing through LWT 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.

Regardless of whether families choose to purchase through LWT or another supplier, all students who are bringing their own device will have access to the same DET programs (eg. Microsoft office) and the school network.

Internet Usage

Student device use is governed by the "Digital Learning – Internet Social Media and Devices policy" which included our Acceptable User Agreement which 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. The use of VPNs and proxy bypass software at school is not allowed. This helps to protect your child and the wider DET system.

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 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 home ready for the commencement of every school 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 school.

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.

Storage of devices at school

Students in Years 7-9 are required to purchase a lock for their locker before bringing their device to school for the first time. Please consider whether a combination lock or key lock would be best suited to your child. Students in Grades 5-6 will be provided a space within their classroom to store their devices during the day. Classrooms will be locked when staff and students are not in spaces.

What students can and cannot do on a laptop whilst on College grounds.

You <u>CAN</u>....

- 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.
- 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 <u>CANNOT</u>...

- 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, FaceTime or any video sharing app whilst on College grounds.
- Use social media apps or websites while at school.
- 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>. Use the laptop appropriately and you will be able to enjoy all the benefits it provides!

<u>Advice for Parents</u>

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. 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, just as it is for offline behaviours, 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.

<u>Bridging the gap between home and school</u>

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

The following resources and links provide a wealth of information (for both parents and students) on a number of topics and issues relating to cybersafety and social networking.

www.digitalthumbprint.com.au/parent-resources
Parents can access a number of resources and useful conversation guides (designed specifically for parents) in a number of topic areas relating to their child's online safety.

www.esafety.gov.au
An absolute smorgasbord of information on all topics and issues relating to social media and cybersafety. It is highly recommended that parents visit the "– parents resources" . The website provides a link to the office of the children's eSafety Commissioner. It allows children to post reports when they are being bullied or have viewed anything online which is illegal or offensive.

Digital/Cyber Safety Tips For Kids
A worthwhile site for parents who want to improve their basic knowledge and practice of online safety with the view of protecting and supporting their children. It contains great tips on how to use the internet safely, easing parent anxiety so that their children can explore and use digital technologies safely. There is a real focus on how to go about educating your children about the risks and dangers associated with the internet and social media, so that they become responsible users and good digital citizens.

www.consumerprotect.com
The risks associated with the use of social media can often outweigh its many benefits. This website outlines the risks and sometimes criminal activity connected to social media platforms. It is an invaluable resource for parents/guardians which assists them in guiding their children in the appropriate and safe use of social media.

www.kidshelp.com.au/teens/get-info/cyberspace
A really good site for children and parents. It contains great tips on how to use the internet safely, easing parent anxiety so that their children can explore and use the Net for education and entertainment. This website also contains invaluable information about cyberbullying and 'sexting'.

http://videogames.org.au
This is a resource website developed by Steve Dupon (Youth Services Manager Manningham YMCA). It is designed for parents and professionals who want to know more about the impact of video games on children. It deals with both the benefits and risks in playing online games and provides support material for parents who are faced with the challenge of 'addiction' in their children.

www.cybersafekids.com.au
A worthwhile site for parents who want to improve their basic knowledge and practice of online safety with the view of protecting and supporting their children.

www.commonsensemedia.org
The "Education" section of this site includes information about a Parent Education Program and lots of resources and ideas for teachers in developing curriculum around digital citizenship.

www.netaddiction.com
Contains information with a focus on the tell-tale signs of internet addiction. It provides valuable resource

material for parents and 'addicted individuals' in seeking treatment/help for internet addiction.

http://www.securedatarecovery.com/resources/personal-data-loss-a-guide-to-identity-theft
The site explains how easily identity theft can happen and outlines the consequences that all online users should be aware of. It also provides some strategies on identity theft prevention.

www.privacy.gov.au/topics/youth
This is an Australian Government site which provides a host of information and resources. There is a focus on social networking and privacy issues. It is recommended that you visit the STAYSMARTONLINE link on this web page (see below).

www.staysmartonline.gov.au
There are great tips and advice for 'kids and teens' on a range of topics including safe social networking, how to deal with cyberbullying, and helpful advice on how to secure your mobile phone.

DET Bully Stoppers Program
This is a Department of Education (DET) resource which provides advice and information for students, parents, teachers and school principals (sorted in categories). It is a good resource for parents who suspect that their child is being bullied, but is not admitting to it.

Australian Council on Children and the Media
A non-profit body committed to promoting a media environment that fosters the health, safety and wellbeing of Australian children. Provides movie and app reviews as well as parent guides and resources about media matters involving children.

Kidspot
Australian parenting website featuring resources and advice about child development issues from pregnancy through to raising teens. Features articles, blogs and parent guides about a range of issues including cybersafety, TV, apps and social media.

Raising Children
An Australian parenting website that offers practical and expert child health and parenting information, tips and tools for children aged 0-15 years. Topic areas cover child development, behaviour, health, nutrition, communication, sleep and safety. The play and learning section offers movie reviews and tips about children's TV viewing.

Parentline Victoria 13 22 89
This is a telephone contact, available 8am – midnight, 7 days a week.
A Department of Education resource which provides a statewide telephone counselling service to parents and carers of children (up to 18 years of age). Parentline is also able to provide contact details for relevant community services.

It is also important for parents to be aware of various software products that support parents in managing their child's online behaviour. For example, such sofware can restrict sensitive personal information from being transmitted online, as well as monitoring the sites your child has been to and if they have entered personal information. There are also time-limiting software to make sure that your child goes online only at certain times and filtering software that block access to sites that you feel are inappropriate.

Refer to the resources listed below. This is obviously not an exhaustive list. Parents are encouraged to research similar products.
www.protectachild.com.au