Broadford Secondary College Student Owned Devices – Guidelines, FAQs and BYOD Agreement

CONTENTS PAGE

1. Technical Specifications

As part of the revised Department of Education and Training guidelines regarding student devices (iPads/laptops/netbooks), families attending Broadford Secondary College now have the option to provide their own device for use within classes.

Broadford Secondary College has worked extensively with staff and students to further integrate student devices within the curriculum, making them a valuable learning tool in the classroom.

In order to ensure connectivity and capability for use in the classroom the following minimum system requirements apply

- The laptop must be capable of running Windows 10 natively (not via virtualisation technologies such as Parallels, VM Ware Fusion or Virtual Box)
- A current series i3 processor (or greater)
- Able to be used in a tablet and laptop form factor
- Must offer up to at least 6 hours of battery life
- Minimum 4Gb of RAM
- Support 802.11AC and 802.1X wireless standards
- Include a HDMI or Display Port
- A physical keyboard that is directly attached to the device.

Recommended specs are as follows;

- Windows 10
- i5 Processor
- Able to be used in a tablet and laptop form factor
- Must offer up to at least 6 hours of battery life
- 8Gb of RAM
- Support 802.11AC and 802.1X wireless standards
- Include a HDMI, Display Port or WiDi technology
- A physical keyboard that is directly attached to the device.

In addition to these minimum requirements, parents/guardians should be mindful of other physical aspects of the device, including:

- Size
- Weight
- Duration of time the device will be used for
- Requirements of particular software

□ Warranty Support

□ Accidental Damage Protection

Software Requirements

As the laptop will not be owned by Broadford Secondary College, we are unable to install some software due to licensing restrictions. These software packages will vary according to the subjects and electives selected by your son/daughter.

Students will be given opportunities to access digital resources that will make up for this limitation, ensuring that your child will not be disadvantaged.

It is the responsibility for all parents/guardians to ensure all software is purchased legally in accordance with the Digital Millennium Copyright Act.

Technical Support Provision

Due to the nature of a “Bring Your Own Device” program, and the variation between different laptop models, Broadford Secondary College can only provide a limited amount of support for connecting student owned devices to the Wireless network.

Should your son/daughter experience any warranty and accidental damage issues, they must be managed by the parent/guardian in contact with the laptop supplier or insurer. Please note that many consumer level suppliers only provide an offsite warranty that is typically one year.

It is the responsibility of the parent/guardian to ensure devices purchased for use at Broadford Secondary College comply with the above specifications – Broadford Secondary College provides no warranties or assurances that devices that do not meet these specifications will be suitable for use within the school.

2. Frequently Asked Questions

Who is responsible for backing up the student device?

It is the responsibility of all students, regardless of the device they use, to ensure they keep a backup of all important files. It is recommended that families utilise an inexpensive USB external storage device for this purpose. Cloud based services are available options and can be an inexpensive choice. The advantage of a cloud-based storage solution is the ability to access their files from anywhere that has an internet connection. There is also the added benefit of not losing important files if the physical USB device is misplaced or damaged.

Do I have to install software?

All students will need to install some software on their laptop to ensure it is ready for use in the classroom. It is the responsibility of each student to complete this installation on their own device. Broadford Secondary College will not image your device or install any software for you.

If your son/daughter is participating in an elective that has a specific software requirement, the student device must have this software installed. If this software has a cost associated, it is the responsibility of the parent/guardian to arrange this purchase and installation prior to use of the software in the classroom.

The Microsoft Office package, and additional software resources, are provided by the Department of Education and Training. Students can acquire this by using Office 365 email account.

Every student will be given access to a library of software that can be made available for use by the student at no extra cost. However, this library of software is by no means extensive and is reliant on the student agreeing to the BYOD Agreement.

Do I need Anti-Virus and Anti-Malware software?

Every device connected to the Broadford Secondary College network must have software installed to protect it against Virus and Malware attack. Microsoft provides the Windows Defender suite, which is suitable for this purpose.

Broadford Secondary College does not recommend the installation of other anti-virus software packages, as they can cause connectivity issues with the school's infrastructure. More devices and increased use of devices (and swapping/sharing of files) Increases risk of malware/virus spreading. There should be some 3rd party anti-virus solution that does not cause problems (Kaspersky is a reliable option)

How do I connect my laptop to the school wireless network?

Details for how to connect your laptop to the school wireless network are available from Technology Support and will be supplied after the device is registered with the school for use in the classroom and a copy of the BYOD Agreement has been signed by a parent/legal guardian and the student.

What is the process for registering my device with Broadford Secondary College?

Each laptop in use at the school needs to be registered. Details regarding this registration process may be found at the end of this document. This agreement needs to be completed, signed where required and returned to the ICT office for the process to commence.

A BYOD device will still be bound by school's ICT Acceptable Usage policy.

How many devices can I connect at school?

A device must be registered with the school prior to use. Each student may only bring and connect one device to the Broadford Secondary College network.

In order for the connection process to commence, students must bring their signed ICT Acceptable Usage policy and their laptop to the ICT office where it will be connected as soon as possible.

Why are there two recommendations for device specifications? Will the minimum requirements by insufficient?

The minimum requirements are a guide for what will be able to run the Operating Software and other programs that will be necessary for a student's ability to participate in the digital learning that will take place in the classroom. However, as time progresses, software requirements change and sometimes need more resources than in previous years. Devices become slow and can struggle to provide effective learning support. A device is an investment and should be considered a long-term learning tool. Although there is no guarantee that any device will be able to offer fast and powerful operation during the student's time at Broadford Secondary, purchasing a device with the recommended specifications will at least provide some insurance against needing to upgrade within a short timeframe due to insufficient hardware resources. As student's progress and take on subjects that may require certain software, they may need more substantial processing power than a 'minimum-spec' device can provide.

3. ICT Acceptable Use Policy

3.1 School Rules for Use of Hardware and Software

- Students are responsible for taking full care of their device.
- All users must log in under their own username and password and correctly log out at the end of each session. Students are responsible for information sent or accessed through their login details.
- Students must not attempt to discover, disclose or use another person's password nor must they reveal their own password to others
- At school, the internet is to be used for school work only and the students must not send unnecessary or inappropriate emails.
- Only devices highlighted on the 'Student Owned Devices' document can be used at the school, and can only be used for school work.
- Students must not tamper with the system setup or add or remove school provided programs/applications without permission
- Games are not to be installed excessively on the device (We understand that the devices are privately owned, however, they are for educational purposes and so should not take up more storage space, or require the deletion of other educational applications in order to be installed)

3.2 College Internet Usage and Conduct

- All students must abide by generally accepted rules of etiquette. They must be polite when communication with other people. This includes not swearing, using inappropriate language or vulgarities.
- All students must respect and not disclose and private, confidential, or personal school or student information they may view or have access to.
- Apart from their name, school and email address, students must not disclose any information about themselves on the internet.
- Students are not to attempt or deliberately access, download, upload, send (including forwarding) or view any unacceptable or illegal material. This includes any content that could be considered racist, sexist, violent, anti-social, pornographic, explicit, vulgar or obscene.
- While the school encourages debate, students are not permitted to engage in libellous criticism *(published false statement)* of peers, teachers, the school, staff, other individuals or organisations. Students who are both directly and indirectly involved (through encouragement) of defamatory, libellous criticism and harassment via an electronic medium maybe subject to disciplinary and/or legal (both civil and criminal) action. This extends to all content posted/submitted on social media websites, blogs, wikis, instant messaging and other publically accessible and restricted access websites.
- Students must understand that actions on the internet are subject to both state and commonwealth and laws, in addition to school discipline policies and procedures. Students' online misconduct may also result in criminal and/or civil legal charges and/or penalties

- Students must check the internet rules of different external groups and always observe these rules.
- Students must observe copyright laws when copying or redistributing another's work. Students must always correctly acknowledge the use of another person's work.
- If students read or see something on the internet which they think is not acceptable, they must tell their teacher, learning group teacher or year level coordinator immediately.
- Students must not use the internet for any commercial purposes such as buying/selling of goods
- Students not use any means including anonymous proxies, online tools or software to bypass internet security to access blocked sites.
- Students may only use the devices' camera to take photographs with the permission of a supervising teacher
- Whilst on school grounds, students will only access the internet via the school's network. Wireless hotspots, phones and other devices must not be used.
- Students must not access or attempt to access any non-authorised part of the school's network.
- Responsible cyber citizenship is promoted and all forms of cyber bullying are prohibited.
- Students may not upload to ma website or distribute electronically any material relating to Broadford Secondary College without permission from the principal.

According to DECD ICT Security, Internet Access and Use, and Electronic Mail and Use policies, students may use the Internet only for learning related activities that are approved by a teacher. They must not cause interference or disruption to other people or equipment, and students may not access or distribute inappropriate material. This includes:

- distributing spam messages or chain letters
- accessing or distributing malicious, offensive or harassing material, including jokes and images
- bullying, harassing, defaming or giving offence to other people
- spreading any form of malicious software (e.g. viruses, worms)
- accessing files, information systems, communications, devices or resources without permission
- using for personal financial gain
- using non-approved file sharing technologies (e.g. Torrent)
- using for non-educational related streaming audio or video (e.g:Snapchat, Facebook Messenger)
- using for religious or political lobbying
- downloading or sharing non-educational material

3.3 Customisation of Equipment

- Students may be permitted to personalise their iPads and install/software subject to the oversight of the ICT Co-ordinator, the ICT Team and the Principal or Deputy Principal. The school retains the right to inspect hardware or block software/apps. All apps/software must be in accordance with the school's AUP policy and good taste. Any breach of this rule will attract penalties under the Code of Behaviour and School Rules.
- School management is the final arbiter of what is appropriate in the circumstances.
- When the school decides to restrict a student's or a class group's usage of the iPad, parents/guardians will be notified in advance. Parents/Guardians agreement will be sought but if a satisfactory outcome cannot be reached, the school reserves the right to ban the student from having the iPad in school and the parents will be required to provide the students with regular textbooks at their own expense.

3.4 Equipment

- Parents/ Guardians are responsible for purchasing the iPad and ebooks/apps for their sons/daughters. They are also responsible for its safe-keeping, repair and insurance. Whilst parents retain ownership and possession of the iPad, they agree to grant to teachers and school principal and Deputy Principal the right to collect and /or inspect and /or confiscate (for a limited period) the iPad at any time and the right to: alter, add, block or delete installed software, apps, hardware, internet access etc.
- All devices must have our MDM (Mobile Device Management) software installed on the iPads. This allows us to control the iPad in a monitored environment in the school.
- MDM software installed on iPads is not to be removed. Students who remove the MDM software will be subject to appropriate disciplinary consequences.
- Usage, within the school is a privilege and not a right. Students may lose their right to use the iPad and to have it in their possession if they abuse their responsibilities and breach this policy, the school AUP and the Code of Behaviour and School Rules.
- The school is invested in delivering ICT learning in the classrooms, and as such, may provide students with technology required to complete work for particular subjects. The student is responsible for the use and maintenance of the technology that is entrusted to them. Therefore, any damage to technology that has been entrusted to the student is the sole-responsibility of the student alone and therefore will be responsible for the replacement or re-conditioning of the damaged technology. Mysterious third-parties will not be accepted as a reason for why the technology was damaged (unless the school is able to verify that the technology was damaged by someone that was not the student responsible for the equipment.)

3.5 Software installation, games and music

- Students may have Administrator access to their iPad/BYOD device and may be permitted to install certain types of software and files provided they have acquired a legitimate license.
- Student installed software must be educational in nature or have a direct relationship to student learning.
- Non-educational software, games and music are not recommended as they will unnecessarily use space on the hard drive and therefore impede use of the device for learning. Students using non-educational software, games and files at school will be subject to consequences according to the 'Acceptable Use' section.
- In instances where the device's performance is restricted due to student installed software and files the device will be reset by IT Services.
- Under no circumstances may software and files be installed without the appropriate license - students doing so will be liable to prosecution.
- Parents/caregivers are encouraged to regularly monitor the contents of the device.

3.6 Training and Development

- Training and development will be provided in order to familiarise students and their parents or caregivers with the device. It is expected that parents/caregivers and students will attend an initial session in order to setup their device. This session will cover:
- Welcome to your device
- Cyber Safety
- Parents/Caregivers use of the device
- Using the device for learning

3.7 Student Activities Strictly Prohibited

- Illegal installation or transmission of copyrighted materials.
- Any action that violates existing school council policy or public law.
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials.
- Inappropriately utilizing photos, video, and/or audio recordings of any person.
- Changing iPad settings in an effort to circumvent the filtering system.
- Downloading inappropriate apps.
- Spamming-Sending inappropriate emails.
- Gaining access to other student's accounts, files, and/or data.
- Vandalism to your iPad or another student's iPad.

4. Meraki Systems Manager

Meraki Systems Manager is a mobile device management solution that allows us to manage multiple iPads quickly and easily from a central location.

Management of devices include:

- The ability to reset PIN if forgotten. A forgotten PIN would usually require the iPad to be wiped, but using Meraki we can avoid losing the contents on the iPad under most circumstances.

- Find the iPad if it has been lost or stolen
- Push out school-provided and free apps on the fly, no purchase needed
- View what is currently installed on the iPad.

Meraki does not allow us to do the following:

- Record the movements of students
- View anything that is contained within Applications (i.e: Photos, emails, etc)
- Delete applications that have been installed via the App Store
- Activate Camera or Microphone
- Access Credit Card details

Computer operating systems and other software have been set up to maximise the usefulness of the iPad. Students are prohibited from:

- Bringing or downloading unauthorised programs, including games, to the school or run them on school computers. Online internet games are banned.
- Deleting, adding or altering any configuration files.
- Break software copyright. Copyright is to be observed at all times. It is illegal to copy or distribute school software. Illegal software from other sources is not to be copied to or installed on the school equipment.
- Deliberately introduce any virus or program that reduces system security or effectiveness.
- Bypassing the school proxy server.
- Attempting to log into the network with any user name or password that is not their own, or change any other person's password.
- Revealing their network password to anyone except the system administrator. Students are responsible for everything done using their accounts and everything on their iPad. Since passwords must be kept secret, no user may claim that another person entered their home directory and did anything to cause school rules to be broken.
- Using or possessing any program designed to reduce network security.
- Enter any other person's file directory or do anything whatsoever to any other person's files.
- Attempting to alter any person's access rights; or storing the following types of files in their home directory:

- Malicious program files
- Compressed files (containing malicious/inappropriate content)
- Picture files, unless they are required by a subject
- Obscene material – pictures or text
- Obscene filenames
- Insulting material
- Copyright material.

5. Social Networks and Chat Lines (Face Book, Tumblr, My Space, twitter, Skype, IRC, MIRC, MSN, ICQ etc)

Real-time chat programs and social networks (Face Book, MIRC, ICQ) may be used at home with the permission of parents however they are not to be used by students in class unless instructed to do so by a teacher.

6. Games and music

Playing games, listening to music, watching video, accessing websites not relevant to the lesson, or any other activity on the connectable device which is a distraction will not be tolerated during class time. This policy will be strictly monitored by the class teacher and remotely by other staff, and action will be taken if this policy is breached. The extent to which the student conducts these activities at home is the decision of the parent, but it is to be remembered the connectable device is primarily to be used as an educational tool. At all times games and audio visual material must not breach the appropriate censorship rating.

7. Privacy

Do not store anything on the iPad that you are not prepared to share with staff or your parents. Student activity on the iPad can be monitored at any time at school using monitoring software, and this may include remotely viewing and taking control of the desktop. School staff may request access to the iPad, including access to the Internet browser history, logs, caches and files and programs stored on the iPad, or Cloud. Staff may also install or delete software. The school cannot monitor use of the iPad outside of the school, and it is the responsibility of the parent to ensure it is used appropriately at home. The student is expected to make their password available to their teachers and parent if they need to examine the iPad. When using online cloud services, all students and staff will practice safe behavior characterized by non-disclosure of sensitive personal information that may be stored in servers outside of Victoria (ie; Google Apps, Office365, etc).

Broadford Secondary College BYOD Agreement

As part of the revised Department of Education and Training, guidelines regarding student devices families attending Broadford Secondary College now have the option to provide their own device (iPad/Laptop/Netbook) for use within classes.

Before any Broadford Secondary College student may bring a device to school, the following agreement must be completed by the student and parent.

STUDENT AGREEMENT

Before you may bring a device to use the network and facilities at Broadford Secondary College, you must sign this contract which binds you to the following conditions as set out in the **ICT Acceptable Use Policy**. If you break any of the conditions, penalties may apply.

In addition, I understand that any device I bring to school must be immediately registered with Technology Support upon arrival to the school, where it will be connected to the network.

Name:

I have read the Guidelines and Conditions for Appropriate Use of ICT Resources document and agree to obey the guidelines and conditions in it.

Signed: ______________________________

Date: ______________________________

PARENT / LEGAL GUARDIAN AGREEMENT

I, the Parent/Guardian of ___________________________________(students Name) have read and understood the **ICT Acceptable Use Policy document**. I agree that my child shall observe these guidelines and conditions

In addition to the stipulations outlined in the documents named above, I understand that I am bound by the following stipulations:

- I understand that the device brought to school by my child may, with my permission, be confiscated by Broadford Secondary College staff in the event of a breach of the ICT Acceptable Usage Policy.
- I understand that if my son/daughter's device is confiscated for any reason, it will be returned to me in person at Reception.
- I will ensure all software required by the school curriculum has all software as instructed and installed on my son/daughter's device prior to commence of the class.
- I understand that any technical support and repair work, excluding connecting the device to the "Broadford Secondary College" network, is solely my responsibility.

Name:

I have read the Guidelines and Conditions for Appropriate Use of ICT Resources document and agree to obey the guidelines and conditions in it.

Signed: ____________________________

Date: ____________________________

Once this document has been signed, please use the device's onboard camera function to take a photo in order to create a digital copy of the signed agreement for digital storage purposes