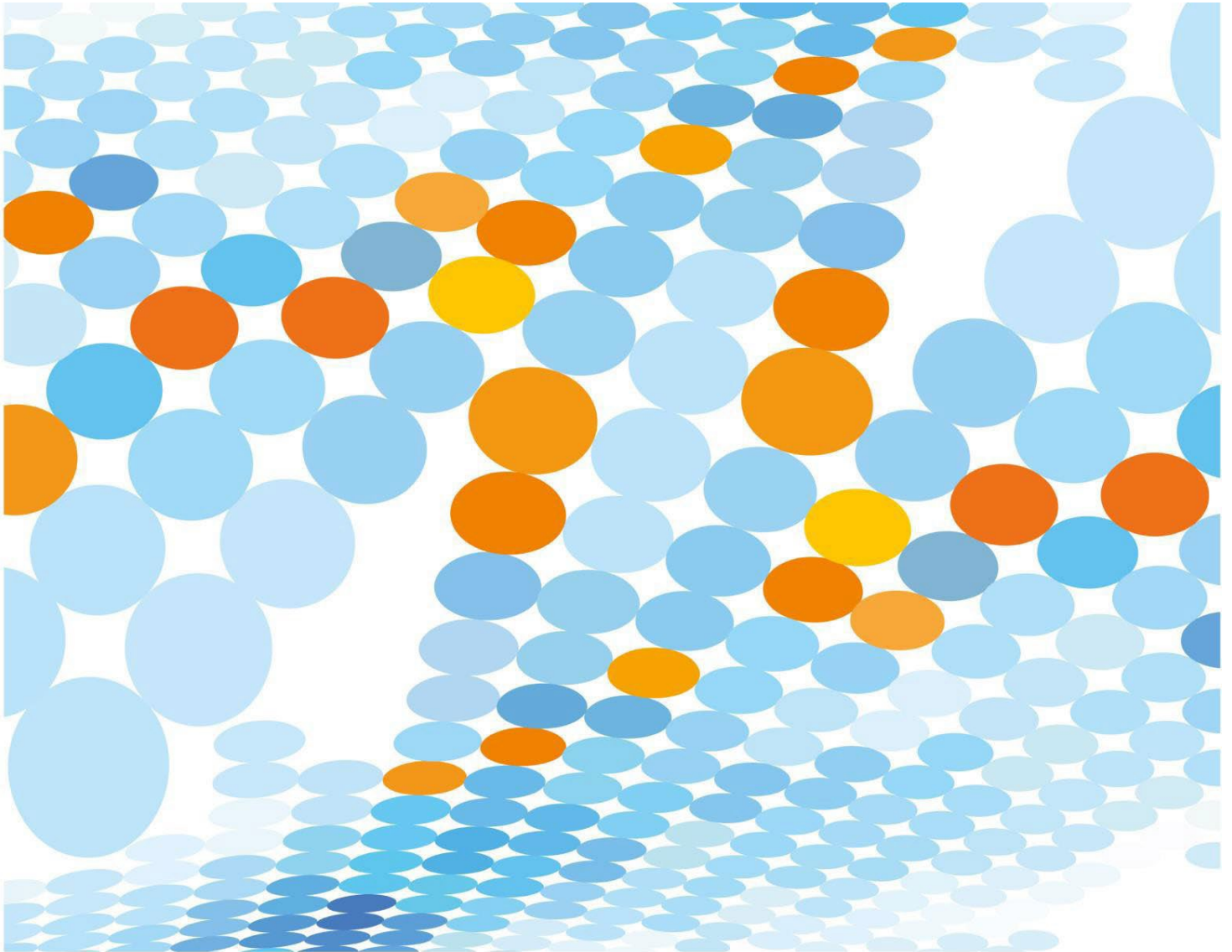


Grand Avenue State School



BYO – iPad

Bring Your Own Device Handbook



Contents

BYO iPad at Grand Avenue State School	4
Overview:	4
What is BYO iPad	4
BYO iPad Program at Grand Avenue State School	4
Initial Wi-Fi Connection - BYOx Link	5
IPAD - BYOxLink - How to guide - iOS – Enrol your BYO iPad into Intune.....	5
Minimum Device Specifications.....	5
Purchasing an iPad for BYO.....	5
Case and Keyboard Requirements.....	6
Software Requirements.....	6
Microsoft Office 365	7
OneDrive for Business	8
With regards to file sharing, students should	8
School vs Personal files.....	8
Syncing files	9
Enrolment status	9
School Technical Support.....	9
School technicians are not able to support students with (but not limited to).....	9
General Care and Acceptable Use.....	10
Use and care of your iPad	10
Protecting the screen	10
Charging of Devices	11
Mobile Data Networks (eg, 3G, 4G, 5G) and Internet Tethering.....	11
Printing	11
Safety and Security	11
Security of Devices.....	12
Passwords.....	12
Cybersafety.....	12
Digital Communication Tools	13
Web Filtering	13
Privacy and Confidentiality	14
Intellectual Property and Copyright.....	14

Data Security and Backups	15
Monitoring of Use.....	15
Internet Use.....	15
Damage or loss of equipment.....	15
Daily Usage	16
Before and After School Usage	16
Lunchtime Usage of iPads.....	16
Outside School Hours Care	16
Misuse and breaches of acceptable usage.....	16
Grand Avenue State School ICT Responsible Use Policy	18
Authorization and controls	18
Responsibilities for using the school's ICT facilities and devices	18
Acceptable/appropriate use/behaviour by a student.....	19
Unacceptable/inappropriate use/behaviour by a student.....	19
Period of Participation	20

BYO iPad at Grand Avenue State School

Overview:

Over the past decade our students, as well as technology, have changed. These fundamental changes impact on what we teach and how students learn. It is therefore important to provide opportunities for students to develop the knowledge, skills and attitudes to prepare for a future in the 21st century. With students having 24/7 access to a digital device, learning will extend from the classroom to wide-reaching resources providing learning anywhere, anytime. With a powerful new tool set, students and teachers are able to engage in valuable new learning experiences. The Grand Avenue State School BYO iPad program has been established with a goal to facilitate a digital learning environment for every student in Years 4 - 6 at both school and home. We must provide students with the opportunity to be effective digital learners who become confident, creative and productive in a digital world.

What is BYO iPad:

“Bring your own”, BYO iPad refers to technology models where students bring a personally owned iPad to school for the purpose of learning. Put simply, BYO iPad is a solution where students quite literally bring their own iPad to school in order to access the Internet and/or school network through a managed Wi-Fi connection. In 2022 Grand Avenue State School will continue to permit a range of devices meeting a certain specification to connect to the school’s wireless network to enable students to learn digitally, as we move towards a full BYO iPad program from 2024.

BYO iPad Program at Grand Avenue State School

The recommended device for Years 4-6 is an iPad. Students with BYO iPads will have access to a filtered Internet connection, access to classroom content, and a connection to

printers within the school. Students and parents/caregivers are asked to lend their support to this very valuable and innovative program. Strong support from parents and caregivers is paramount to ensuring the program is successful and that students gain maximum benefit for their learning.

Initial Wi-Fi Connection - BYOx Link

All iPads must be set up at home before they can be used within the school. This procedure preloads the iPad with the wireless configuration so that the iPad will connect automatically when onsite. The following links contain videos on how to set up your child's iPad for use with the school. If you are unsure of your child's email address or password, then please make contact with their class teacher.

IPAD - BYOxLink - How to guide - iOS – Enrol your BYO iPad into Intune

<https://mediasite.eq.edu.au/mediasite/Play/bbe46710d2c24274a0a99cba446a92031d>

Minimum Device Specifications:

In order to provide a consistent experience for students, it is important the iPad meets the minimum standards recommended by our school, this will ensure the device is able to connect to the school network, to connect to our printing systems, and ensures that digital content used in the classroom is compatible with the chosen device. Please do not purchase an iPad unless you are sure the iPad meets the specifications.

Purchasing an iPad for BYO:

The BYO iPad program relies heavily on the desire for students to bring their iPad to the school on a daily basis. It is a good idea to purchase the iPad early so the student can become familiar with it and hit the ground running when they start in the new year. Please read the BYO section of our website to ensure your iPad meets the required specifications. This “live” section of the website allows us to provide updated information as iPads are added to the compatibility list.

When purchasing an iPad, it is important to consider future technical support requirements. As part of the BYO iPad Program, technical support is provided for connectivity issues in

connecting iPads to the school network. We are unable to provide technical support beyond this.

The school strongly recommends that families seek and provide their own warranty and insurance (accidental damage) protection for all iPads. Grand Avenue State School cannot be held responsible for any damage to the iPad. Please note that the school will take all reasonable steps to connect BYO iPad's, however it cannot take any responsibility if we are unable to connect an iPad to our network.

Please investigate any tax rebate eligibility to ensure that you receive any credit to which you are entitled.

Should you have any specific questions in regards to a particular iPad specification then please complete the pre-purchase checklist and email it to BYO@Grandavenuess.eq.edu.au or contact the school for assistance.

Case and Keyboard Requirements

All students are required to have a robust protective case which contains a keyboard for their iPad.

A case is required as well as a protective sleeve or pouch. The case must protect the iPad from damage in the event it is dropped. The keyboard is important as this will be used for specific curriculum work which requires access to a keyboard. An iPad sleeve or pouch goes over the case and is essential to protect the device when in transit in the school bag and should adequately protect and prevent the iPad from being exposed to the elements.

Devices should always remain in their protective cases (and sleeve) during transport between classes and between school and home. When not in use they should also be in their protective case.

Students are expected to have name labels placed on the following locations:

- A name label easily visible on the case of the iPad.
- A key tag for the protective sleeve/pouch/case for ease of identification.

Software Requirements:

Software installation, with the exception of software packages distributed by Grand Avenue State School, is the responsibility of the student/parents/caregivers. Valid licenses are required for all software present on your iPad.

A core set of applications will need to be installed on each iPad as well as specific year level applications. A list will be available on the “Comp Portal” (Microsoft Intune Company Portal) App and automatically updated each year.

It is critical that these applications are loaded onto your iPad before it is brought into the school. Without all applications present your child will not be able to operate effectively in class. If apps are missing the student may be advised to not bring the iPad again until they have been installed.

It is important that all iPads have at least 2GB free (as a recommendation) at all times to ensure that there are no issues associated with a lack of free space on the iPad.

It is essential that students have created a passcode / password for their iPad and that this remains known to only them, to ensure the security and safety of their iPad and their work.

Apple - [Use a passcode with your iPhone, iPad or iPod touch – Apple Support \(AU\)](#)

Students may install or have parents install other applications onto their iPad. Please remember that Apple do not permit students under the age of 13 to create an Apple account. Students may have games or other apps on their iPad, but they are not permitted to use these during school hours. We recommend that families make use of Apple’s Family Sharing and Screen Time features so that apps can be shared amongst siblings and so that parental controls can be established to limit screen time where appropriate.

Apple - [Use parental controls on your child's iPhone, iPad and iPod touch – Apple Support \(AU\)](#)

It is important that there is no illegally downloaded media or software on the iPad.

iPads are never to be used to engage in illegal activity, including violation of copyright or other contracts.

Microsoft Office 365:

A Microsoft Office 365 licence is available to all students at no cost. Microsoft Office 365 contains the products Word, Excel, PowerPoint, Outlook (desktop and online version), OneNote and access to OneDrive. Details on how to install, access and use can be found here:

<http://education.qld.gov.au/learningplace/help/home-computer-support.pdf>

OneDrive for Business:

Students can only share files with people who have an @eq.edu.au email address. This includes staff and students. To share a file, students will need to type the user's full @eq.edu.au email address.

With regards to file sharing, students should:

- Only share files with people that they know.
- Edit the sharing permissions to 'Specific People', so only people with whom the link is shared can access the file.
- Check they have entered the email address accurately before sharing.
- Only open files that have been shared with them by someone they know; and
- Alert their teacher if they think someone has accidentally shared a file with them, or someone has shared files that are not appropriate.

School vs Personal files

Students should only use OneDrive to share school related files. School related files include those that are created for the purpose of completing a class activity or an assignment.

Students should ask themselves, 'Would I get in trouble or be embarrassed if my teacher saw this file?' If the answer is 'yes', then it is likely that the file should not be stored in the student's OneDrive. Examples of files that would not be appropriate to store in OneDrive, include:

- Your personal journal or diary (excluding one written as part of a class activity or assignment)
- Your contact list (e.g., you or your friends' addresses, emails, phone numbers, photos etc.)
- Account credentials (e.g., social media usernames and passwords)
- Personal photos and media (e.g., video or sounds files of you, your family and friends).

- Games (excluding assignment related projects)
- Your personal movie or television collection.
- Illegally downloaded media (movies, music, television shows etc.) or software.

Students should check with their teacher/s if they are not sure whether a file should be stored in OneDrive.

Syncing files

Use of OneDrive can affect the school's internet speed. To avoid negative impacts, students should avoid:

- Uploading large files, or large numbers of files to their OneDrive library during school hours
- Inserting large images or attachments directly into OneNote Notebooks or Class Notebooks.

Enrolment status

When a student's enrolment status changes (eg. following move to non-state school, Year 12 graduation), they will no longer be able to access their @eq.edu.au email or OneDrive library. Students must backup any files/emails they wish to keep prior to leaving the school.

School Technical Support

School technicians will assist students in the BYO program with the connection of their device to the school network and any ongoing connection issues. Because of the range of devices able to be used within the school, technical support is limited to:

- Connection of the device to the school wireless network
- Connection of the device to the school printers

School technicians are not able to support students with (but not limited to):

- Hardware faults
- Software issues
- Physical damage to your device
- Issues caused by viruses. (It is important to note that where a device potentially threatens the school network, it may be temporarily or permanently suspended from connecting).

Students are to contact their teacher if they require technical support or are experiencing any issues.

General Care and Acceptable Use

Students are responsible for the general care of their device.

Use and care of your iPad:

- Bring your iPad to school each day fully charged.
- Hold your iPad with two hands when carrying it.
- It is recommended that food and drinks should not be near your iPad when in use.
- Plugs, cords, and cables should be inserted and removed carefully.
- iPads should be carried within their protective case where appropriate.
- Turn the iPad off before placing it in its bag.
- iPads should never be left unsupervised.
- Students are responsible for ensuring the battery is charged for school each day
- Avoid dropping or bumping your iPad.
- Don't place your iPad in areas that may get very hot.
- Don't allow iPad to get wet. Even though they may dry and appear to operate normally, the circuitry could slowly corrode and pose a safety hazard.
- Follow all instructions given by staff.
- Avoid exposing your iPad to direct sunlight or sources of heat such as desk lamps, dust, dirt, rain, liquids or moisture, heavy shock, or vibration

Protecting the screen

- Avoid putting excess pressure on the screen with your hands.
- Do not place anything near the iPad that could put pressure on the screen.
- 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.
- Don't clean the screen with a household cleaning product.

Charging of Devices

Students will not have the opportunity to charge their device during class and it is expected that devices used within the school have sufficient battery power to last an entire day. Your device is to be fully charged before the commencement of each school day.

Mobile Data Networks (eg, 3G, 4G, 5G) and Internet Tethering

Mobile network tethering, wireless internet access points and inbuilt data connectivity can provide students with an UNFILTERED network connection within the school grounds. These types of internet connections need to be disabled before arrival at school as the school cannot monitor or take responsibility for content accessed via these methods.

Printing

Students will be able to print via PaperCut Mobility print, which emulates Apple air print services. Students begin each term with \$5 printing credit (approximately 250 B&W A4 prints) assigned to their account.

Safety and Security

Students are responsible for the security and use of their device whilst at school.

Security of Devices

Students are to remain with their iPad at all times, and they are only to be used in class with the support of their teacher. Students may take the sleeves/pouches containing their device into classrooms once their teacher has opened the classroom for the day. Students must otherwise stay with their bag and iPad. Under no circumstances should iPads be left unsupervised.

Passwords

Each student at Grand Avenue State School has their own unique user account. Passwords must not be obvious or easily guessed. They must be kept confidential and changed when prompted or when known by another user. Personal accounts cannot be shared. Students should not allow others to use their personal account for any reason. When using desktop computers, students should log off at the end of each session to ensure no one else can use their account.

Cybersafety

At any time, if a student believes they have received a computer virus or spam (unsolicited email), or they have received a message that is inappropriate or makes them feel uncomfortable, they must inform their teacher, parent and/or caregiver as soon as possible.

Students and parents are encouraged to explore and use the Government's e-safety website to understand, take appropriate precautions and learn how to deal with any cybersafety issues. You can find this information at the link below:

<https://www.esafety.gov.au/>

Parents are also encouraged to visit and explore the Government iParent website for guidance with using safety settings on your family's web-connected devices, tips for choosing movies and games and strategies for keeping young people safe online.

<https://www.esafety.gov.au/parents>

Students must 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 messages, 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 or publish:

- Unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
- Sexually explicit or sexually suggestive material or correspondence.
- False or defamatory information about a person or organisation.

Students must not engage in cyberbullying, which may include threats, bullying or harassment of another person. Cyberbullying, regardless of where it happens, will be dealt with in accordance with Education Queensland's Policies and incidents will be reported to the police where required.

Digital Communication Tools

For BYO iPads, we require that instant messaging and audio / video communication features are not used within the school, (as outlined in the BYO rules for students) which includes but is not limited to Skype, Facebook, Snapchat, TikTok or iMessage. No attempts should be made to use such services on BYO iPads within the school or whilst connected to the DET network.

Web Filtering

An internet filtering solution provides DET with the ability to restrict access to inappropriate material on DET's network. Content filtering is active only whilst the device is connected to the school's wireless network. To help keep students safe, we do not permit students to use their

own 3G or 4G mobile data connection whilst on campus. Any content accessed in this manner will not be filtered.

It is important to remember filtering systems are not foolproof and do not replace the need for care when students are online. Parents, caregivers and students are encouraged to visit the e-safety site listed previously above to learn more.

Students must not use VPN software or similar to bypass or attempt to bypass filtering restrictions.

Privacy and Confidentiality

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.

The student should not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others.

Students must not record, photograph or film any students, teachers or school personnel without the express permission of the supervising teacher. Identifying images, audio content and personal information must not be uploaded to the internet or leave the school (this information may be saved on the school server only).

It should also be ensured that privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interest.

Intellectual Property and Copyright

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

Data Security and Backups

Students must understand the importance of backing up data securely. Should a hardware or software fault develop, assignment work that has taken a considerable time to prepare may be lost.

The student is responsible for the backup of all data. While at school, students are able to save data to their personal OneDrive account. They are also able to save data locally to the 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 external hard drive or “cloud” based storage.

Students should also be aware that, in the event that any repairs need to be carried out, the contents of the device may be deleted when the device is repaired / replace by your products vendor.

Monitoring of Use

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, DET will comply with all legislative requirements.

Internet Use

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

Damage or loss of equipment

iPads are used within the school at your own risk. It is important to ensure that devices are insured against theft, damage or loss in order to avoid unexpected expenses. Many home insurance policies allow you to specify coverage for mobile devices and we strongly

recommend taking advantage of this. Any software or hardware issues, vandalism, damage, loss or theft of the device must be reported immediately to the school. Devices with dangerously cracked screens are not to be used within the school.

Daily Usage

Unless specifically advised otherwise by their teacher, students are required to bring their iPad every day. iPads will only be used when they are best fit for current learning outcomes. No other student will be permitted to nor should be using your child's device within the school.

Before and After School Usage

Students are not permitted to use their iPad on school grounds before or after school without the express permission of a teacher and under their direct supervision. iPads are not to be removed from school bags until students are in their classroom and their teacher has directed them to do so.

Lunchtime Usage of iPads

Students are not to use their iPad at lunch unless arranged and supervised by a teacher

Outside School Hours Care

Students who attend Outside Hours School Care should follow the directions of supervisors and follow all school procedures. iPads should only be used in designated areas for homework purposes if permitted to do so.

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.

The misuse of Internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services and/or device.

Grand Avenue State School ICT Responsible Use Policy

Upon enrolment at Grand Avenue State School, all students and parents/caregivers are required to sign the Grand Avenue State School ICT Responsible Use Policy.

This policy also forms part of this agreement. The Responsible Use Policy conditions apply to the use of the devices and Internet both on and off the school grounds.

Communication through the Internet and online communication services must also comply with the Student Code of Conduct which is available on the school website.

Authorization and controls

The principal reserves the right to restrict student access to the school's ICT services, facilities and devices if access and usage requirements are not met or are breached. However restricted access will not disrupt the provision of the student's educational program. For example, a student with restricted school network access may be allocated a stand-alone computer to continue their educational program activities.

The Department of Education monitors access to and use of its network. For example, email and internet monitoring occurs to identify inappropriate use, protect system security and maintain system performance in determining compliance with state and departmental policy.

The department may conduct security audits and scans and restrict or deny access to the department's network by any personal mobile device if there is any suspicion that the integrity of the network might be at risk.

Responsibilities for using the school's ICT facilities and devices

- Students are expected to demonstrate safe, lawful and ethical behaviour when using the school's ICT network as outlined in the Student Code of Conduct.
- Students are to be aware of occupational health and safety issues when using computers and other learning devices.

- Parents/guardians are also responsible for ensuring students understand the school's ICT access and usage requirements, including the acceptable and unacceptable behaviour requirements.
- Parents/guardians are responsible for appropriate internet use by students outside the school environment when using a school-owned or school-provided mobile device.
- The school will educate students regarding cyber bullying, safe internet and email practices, and health and safety regarding the physical use of ICT devices. Students have a responsibility to adopt these safe practices.
- Use of the school's ICT network is secured with a username and password. The password must be difficult enough so that it cannot 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).
- Students cannot use another student's or staff member's username or password to access the school network. This includes not browsing or accessing another person's files, home or local drive, email or accessing unauthorised network drives or systems. Additionally, students should not divulge personal information (e.g. name, parent's name, address, phone numbers), via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school.
- Students need to understand that copying software, information, graphics, or other data files may violate copyright laws without warning and be subject to prosecution from enforcement agencies.

Acceptable/appropriate use/behaviour by a student

It is acceptable for students while at school to use a device as listed below:

- assigned class work and assignments set by teachers
- developing appropriate literacy, communication and information skills
- authoring text, artwork, audio and visual material for publication on the intranet or internet for educational purposes as supervised and approved by the school
- conducting general research for school activities and projects
- communicating or collaborating with other students, teachers, their parents or experts in relation to school work
- accessing online references such as dictionaries, encyclopedias, etc.
- researching and learning through the department's eLearning environment
- being courteous, considerate and respectful of others when using a device as directed by the teacher.

Unacceptable/inappropriate use/behaviour by a student

It is unacceptable for students while at school to:

- use a mobile device in an unlawful manner
- download, distribute or publish offensive messages or images
- use obscene, inflammatory, racist, discriminatory or derogatory language
- use language and/or threats of violence that may amount to bullying and/or harassment or stalking
- insult, harass or attack others
- deliberately waste printing and internet resources
- damage computers, printers or network equipment
- commit plagiarism or violate copyright laws
- ignore teacher directions regarding the use of social media, online email and internet chat
- send chain letters or spam email
- share their own or others' personal information and/or images which could result in risk to themselves or another person's safety
- knowingly download viruses or any other programs capable of breaching the department's network security
- use in-built cameras inappropriately, such as in change rooms or toilets
- invade the privacy of others by recording personal conversations or daily activities and/or the further distribution (eg. forwarding, texting, uploading) of such material
- use the mobile device to cheat during exams or assessments.

Period of Participation

The school agrees to provide access to the student/caregiver from the date soon after this agreement is signed by all parties and arranged payment schedules are met.

The agreement may be ended earlier, at the school's absolute discretion, if:

- The student is no longer enrolled at the school.
- The student is excluded from the school.
- The parent and/or caregiver fails to comply with the BYO Rules for Students, the school's ICT Responsible Use Policy or the Student Code of Conduct.
-

Contact Information

For all enquiries regarding this program, please contact: BYO@grandavenues.eq.edu.au