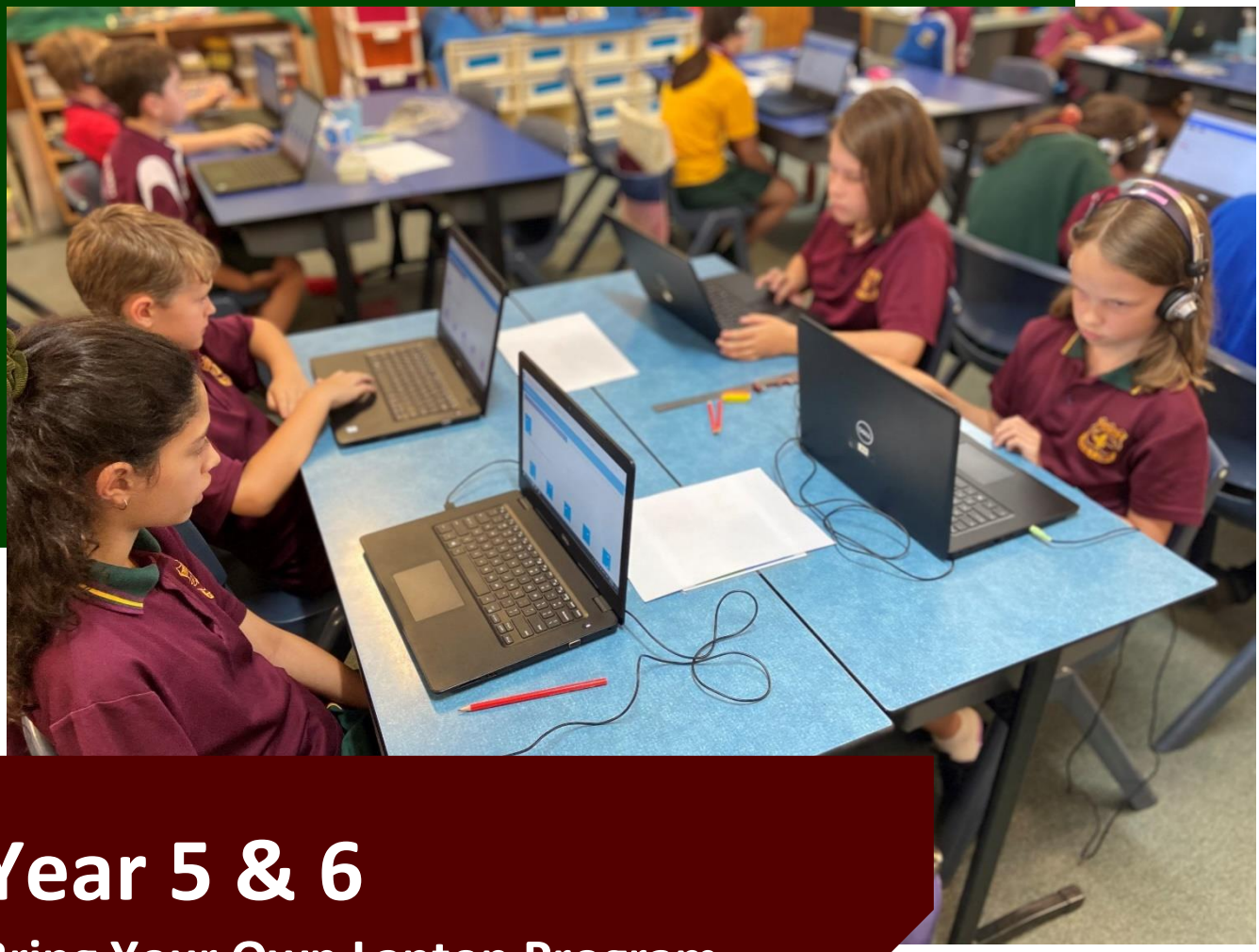
BYOD



Year 5 & 6

Bring Your Own Laptop Program

Buderim Mountain State School

'Strive to Achieve'

Bring Your Own Device (BYOD) 1:1 Laptop Program
Digital Learning Program for Year 5 & 6 Students

Technology at Buderim Mountain State School

Buderim Mountain State School enriches 21st century education delivery through the use of technology in all classrooms across the school. We offer a 1:1 Laptop program in Year 5 & 6, which assists to promote the intentional use of digital technology to enhance teaching, facilitate the creation and sharing of knowledge and allow for additional opportunities to differentiate learning for all students. Buderim Mountain State School strongly believes that students must be exposed to a balance between learning with technology and traditional methods; including pen/pencil and paper. Our BYOD program ensures that students continue to use pen/pencil and paper, be involved in hands-on learning and be engaged in cooperative learning with their teachers and peers, as well as using technology in their day-to-day learning.

The use of a laptop and other technologies:

- Enhances independence and self-initiated learning among students
- Extends student learning beyond the classroom
- Promotes the development of 21st Century teaching and learning
- Enables the delivery of ICT as an Australian Curriculum general capability

Buderim Mountain State School's technology infrastructure has continually evolved over the past decade. Whilst devices have been available for students in the form of desktop computers, iPads and laptops, BYOD fulfils the personalised mobile device experience for student learning in today's progressive digital culture. Teaching staff utilise activities and processes with technology to transform learning experiences to be even more rigorous, relevant, collaborative and engaging for students.

Research

According to John Hattie's study on the practices in schools that have an influence on student achievement, 1 to 1 laptop programs have been found to have a positive influence on student results.
BYOD programs are now becoming common in Australian schools, in particular high schools. The advantage of Year 5 & 6 students accessing a BYOD program in their senior years of primary schooling, is that they will be well prepared in the skills required for secondary schooling.

Research also states that 1 to 1 Laptop programs assist to:

- Facilitate a differentiated, problem-based learning environment demanding higher-order thinking skills
- Foster more collaborative, inquiry-based learning
- Provide timely, more equitable access to a broader range of digital educational resources
- Enable the development of computer literacy skills
- Prepare students to better compete in technology-rich workplaces

We look forward to your children using their own device in Year 5 & 6 to take their learning to the next level.

Contents

Laptop Minimum Requirements

Device selection

Before purchasing a device to use at school, the parent or caregiver and student needs to be aware of the school's minimum specifications of appropriate device type, operating system requirements and software.

Hardware	Minimum	Medium	High
Operating System	Windows 10 (64-bit)	Windows 11	Windows 11
Processor	Quad Core Intel Core i3 \ AMD A6 – Ryzen 3 or equivalent	Intel Core i5 processor or equivalent	Intel Core i7 – i9 or equivalent
CPU Max Speed	2.0Ghz	2.5Ghz	3.0Ghz
Memory (RAM)	8GB	8GB	16GB
Storage Capacity (Hard Drive)	128GB SSD	256GB SSD	256GB & higher
Screen Size	11" display	12" display	12" display or higher
Graphics	256MB	1GB	2GB
Wireless Connectivity	802.11ac Wi-Fi (support of 5GHz wireless range is essential)		
Battery Life	At least 6 hours		
Speakers	Integrated Speakers		
Ports	At least 2 USB ports, microphone and headphone ports.		
Warranty & Insurance	3 Years – accidental damage insurance coverage.		
Accessories	Device protection plans (both warranty and accidental damage) are strongly recommended with all laptops and should be discussed at time of purchase. • Protective case/cover • Padded school bags (laptop friendly) Mouse		

Considerations:

- If your child is planning on attending a private high school, we recommend that parents refer to appendix 4 of this handbook and if needed make contact with our school to discuss BYOD participation options if the destination private school includes a laptop as part of school fees.
- At Buderim Mountain State School, we prefer students use Windows based laptops to assist with classroom curriculum delivery and Education Queensland network connectivity, however if parents are wanting their child to use an Apple MacBook laptop, parents need to make contact with the Deputy Principal to discuss options and required specifications.
- **Our BYOD program does not support the use of iPads or Chromebooks.**

These minimum requirements align with our feeder State High Schools' BYOD Programs (Maroochydore SHS, Chancellor SC and Mountain Creek SHS) to allow students to transition with their device into secondary schooling. Please access the secondary school links for further details.

Safety

Laptop Care

The student is responsible for taking care of and securing their device and accessories in accordance with school policy and guidelines. Responsibility for loss or damage of a device at home, in transit or at school belongs to the student. We recommend that parents look into including their child's laptop in home and contents insurance policies. It is advised that accidental damage and warranty policies are discussed at point of purchase to minimise financial impact should an incident occur.

General precautions

- Food or drink should never be placed near the device.
- Plugs, cords and cables should be inserted and removed carefully.
- Devices should be carried in a protective case where appropriate.
- Carrying devices with the screen open should be avoided.
- Ensure the battery is fully charged each day.
- Turn the device off before placing it in its bag.

Protecting the screen

- Avoid poking at the screen — even a touch screen only requires a light touch.
- Don't place pressure on the lid of the device when it is closed.
- Avoid placing anything on the keyboard before closing the lid.
- 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.

Warranty

We strongly advise that laptops are purchased with at least a 3 year warranty and also include accidental damage insurance to minimise financial impact and disruption to learning should a device not be operational.

Data Security and Back-ups

Students use One Drive to store all school-based documentation. Students must ensure they have a process for backing up their personal data that is not saved on One Drive. Otherwise, should a hardware or software fault occur, documentation may be lost. The student is responsible for the backup of all data.

Passwords

Use of the school's ICT network is secured with a username and password. The password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not revealed to other individuals. The password should be changed regularly, as well as when prompted by the Department of Education's network.

Students should log off at the end of each session to ensure no one else can use their account or device. Students should also set a password for access to their device and keep it private.

Parents/caregivers may also choose to maintain a password on a personally-owned device for access to the device in the event their child forgets their password or if access is required for technical support.

Cyber Safety

If a student believes they have received a computer virus, spam (unsolicited email), or they have received a message or other online content that is inappropriate or makes them feel uncomfortable, they must report this to their teacher, parent or caregiver as soon as possible. Students must also seek advice if another user seeks personal information, offers gifts by email or asks to meet a student. Students are encouraged to explore and use the 'Cyber safety Help button' to talk about, report and learn about a range of cyber safety issues. Students must never initiate or knowingly forward emails, or other online content, 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, post or publish:

- Inappropriate or unlawful content which is offensive, abusive or discriminatory.
- Threats, bullying or harassment of another person.
- Sexually explicit or sexually suggestive content or correspondence.
- False or defamatory information about a person or organisation.

Parents, caregivers and students are encouraged to read the department's Cybersafety and Cyberbullying guide for parents and caregivers.

Web Filtering

The internet has become a powerful tool for teaching and learning, however students need to be careful and vigilant regarding some web content. At all times students, while using ICT facilities and devices, will be required to act in line with the requirements of our school's Student Code of Conduct. To help protect students from malicious web activity and inappropriate websites, the Department of Education operates a comprehensive web filtering system. Any device connected to the internet through the school network will have filtering applied.

The filtering system provides a layer of protection to students against:

- Inappropriate web pages
- Spyware and malware
- Peer-to-peer sessions
- Scams and identity theft.

This purpose-built web filtering solution takes a precautionary approach to blocking websites including those that do not disclose information about their purpose and content. The school's filtering approach represents global best-practice in internet protection measures. However, despite internal departmental controls to manage content on the internet, illegal, dangerous or offensive information may be accessed or accidentally displayed. Teachers will always exercise their duty of care, but avoiding or reducing access to harmful information also requires responsible use by the student. Students are required to report any internet site accessed that is considered inappropriate.

The personally-owned devices have access to home and other out of school internet services and those services may not include any internet filtering. Parents and caregivers are encouraged to install a local filtering application on the student's device for when they are connected in locations other than school. Parents and caregivers are responsible for appropriate internet use by students outside the school.

Privacy and Confidentiality

Students must not use another student or staff member's username or password to access the school network or another student's device, including not trespassing in another person's files, home drive, email or accessing unauthorised network drives or systems.
Additionally, students should not divulge personal information via the internet or email, to unknown entities. It is important that students do not publish or disclose the email address of a staff member or student without that person's permission. Students should also not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. They should ensure that privacy and confidentiality is always maintained.

Monitoring and Reporting

Students should be aware that all use of internet and online communication services can be audited on their device by a staff member when required.

All material on the device is subject to audit by authorised school staff. If at any stage there is a police request, the school may be required to provide the authorities with access to the device and personal holdings associated with its use.

Web Based Services Consent

Permission to Use Cloud, Web Based and App Services

Buderim Mountain State School has audited its use of Cloud, Web Based and App Services across the school and these are listed in our Third Party Web Based Permission Form (Appendix 4), which all parents have been requested to read and either provide consent or not for their child to access these websites. Examples of these services include: Spelling City and Mathletics. All web-based services in use have undergone a risk assessment by the Queensland Government. Teachers in charge of these activities will monitor use and immediately cancel the activity should any concern be raised. Students and parents are asked to report any concerns with any web-based activity to their classroom teacher immediately. Please access the following weblink to provide consent for your child to access third party websites at school. https://survey.qed.qld.gov.au/n/e98h2M6

Behaviour Expectations

Digital Citizenship

Students should be conscious creators of the content and behaviours they exhibit online and take active responsibility for building a positive online reputation. They should be conscious of the way they portray themselves, and the way they treat others online. Students should be mindful that the content and behaviours they create and demonstrate online are easily searchable and accessible. This content may form a permanent online record into the future. Interactions within digital communities and environments should mirror normal interpersonal expectations and behavioural guidelines, such as when in class or the broader community. Parents are requested to ensure that their child understands this responsibility and expectation. The school's Student Code of Conduct also supports students by providing school related expectations, guidelines and consequences.

Acceptable Use

Upon enrolment in a Queensland Government school, parental or caregiver permission is sought to give the student(s) access to the internet, based upon the policy contained within the Acceptable Use of the Department's Information, Communication and Technology (ICT) Network and Systems (Appendix 2). This policy also forms part of this Student Laptop BYOD Program. The acceptable-use conditions apply to the use of the device and internet both on and off the school grounds.

Communication through internet and online communication services must also comply with the school's Student Code of Conduct available on the school website.

Intellectual Property & Copyright

Students should never plagiarise information and should observe appropriate copyright clearance, including acknowledging the original author or source of any information, images, audio etc. used. It is also important that students obtain all appropriate permissions before electronically publishing other people's work. Material being published on the internet or intranet must have the approval of the classroom teacher and have appropriate copyright clearance.

Misuse and Breaches of Acceptable Usage

Students should be aware that they are held responsible for their actions while using their laptop, 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 inappropriately.
The school reserves the right to restrict/remove access of personally owned mobile devices to the intranet, internet, email or other network facilities to ensure the integrity and security of the network and to provide a safe working and learning environment for all network users. The misuse of personally owned mobile devices may result in disciplinary action which includes, but is not limited to, the withdrawal of access to a student's laptop at school and school supplied network services.

Student User Guide

BYOD – Conditions of Use

When using a privately owned laptop at Buderim Mountain State School, we agree that:

- The device must at all times be connected to the school's network when on the school's premises. When connected to the school's network, all activities will be logged. Buderim Mountain State School's ICT guidelines are to be followed in accordance with the completed and signed ICT Agreement (signed on enrolment). (Appendix 2)
- The device will only be used for educational purposes when connected to and using the school's services.
- Buderim Mountain State School will only provide technical support to enable connectivity to the school's network that provides access to student files required for class, internet and printing services.
- It is the responsibility of the student to ensure that their laptop is secured when not in use. Buderim Mountain State School takes no responsibility for the costs in the event of theft, loss, vandalism, damage or unauthorised access to private laptops.
- All private laptops must be brought to school fully charged.
- BYOD devices must contain a virus scanner with up-to-date data virus definitions.
- It is the responsibility of the student to back up data on their laptop e.g. to an external hard drive or USB.
- If your child leaves Buderim Mountain State School, all software purchased under Education Queensland agreements must be removed from the private laptop as per the conditions of the agreement.
- Any privately owned software installed on the laptop must be age appropriate, follow copyright legislation and not cause offence.
- Buderim Mountain State school and the Department of Education reserves the right to restrict access and use of any private laptop used on school grounds, whether it is connected to the school's network or not. Access to the school network and permission to use the private laptop on school grounds will be withdrawn as a consequence of any inappropriate use and/or security breach.
- One Drive is the Department of Education's approved cloud service. Cloud Based Services such as iCloud or Dropbox must not be used at school to store, send or access information at school.

Note: If the above device is substituted, a new IT Permissions and BYOD Connection form will need to be completed and signed prior to connection of the new device.

Security of BYOD, Damage/Theft Insurance, Behaviour

Suggestions about ensuring the laptop is safe at school include:

- Storing the laptop in secure locations determined by your classroom teacher.
- Consider engraving the device – Engraving the bottom of the laptop with the student's name

i.e. First Name and Surname will help staff to locate misplaced laptops and return them to their owners.

- Consider purchasing a small travel padlock to secure your child's bag.
- Home and Contents Insurance – Check with your Home and Contents Insurance company regarding damage or theft of the device.
- Inappropriate Behaviour – While Buderim Mountain State School will continue to manage inappropriate behaviour involving laptops in line with existing policies, the school is not liable for any damage or replacement costs incurred while the device is at school or travelling to and from school.

BYOD Agreement

Our goal is to ensure the safe and responsible use of facilities, services and resources available to students through the provision of clear guidelines.

Responsibilities of stakeholders involved in the BYOD program:

School

- BYOD program induction — including information on connection, care of device at school, workplace health and safety, appropriate digital citizenship and cybersafety
- Providing learning experiences for students on cyber bullying, safe internet and email practices and health and safety regarding the physical use of electronic devices
- Network connection at school
- Applying Student Code of Conduct breaches in cases of intentional damage/Theft and misuse.
- Internet filtering (when connected via the school's computer network)
- Some technical support (internet connection, installing school supported software)
- Some school-supplied software e.g. Microsoft Office 365
- Printing facilities

Student

- Participation in BYOD program induction
- Acknowledgement that core purpose of device at school is for educational purposes
- Care of device
- Appropriate digital citizenship and online safety
- Security and password protection — password must be difficult enough so as not to be guessed by other students and is to be kept private by the student.
- Maintaining a current back-up of data not on One Drive (recommendation each week)
- Charging of device at home
- Abiding by intellectual property and copyright laws (including software/media piracy)
- Ensuring personal login account and device will not be shared with other students.
- Understanding and completing the online acknowledgement of the BYOD Agreement.

Parents and caregivers

- Read through the information and procedures handbook and view the frequently asked questions videos via the school website.
- Acknowledgement that core purpose of device at school is for educational purposes
- Internet filtering (when not connected to the school's network)
- Encourage and support appropriate digital citizenship and cybersafety with students
- Some technical support (technical issues involving hardware and non-school software)
- Required software, including sufficient anti-virus software
- Protective backpack or case for the device
- Adequate warranty and insurance of the device
- Understanding and completing the online acknowledgement of the BYOD Agreement.

The following are examples of responsible use of devices by students:

Use laptops for:

- Engagement in class work and assignments set by teachers
- Developing appropriate knowledge, skills and behaviours
- Authoring text, artwork, audio and visual material for publication on the Intranet or Internet for educational purposes as supervised and approved by school staff
- Conducting general research for school activities and projects
- Communicating or collaborating with other students, school staff and if applicable, experts as part of assigned school work.
- Emailing other students about school related matters.
- Accessing online references such as dictionaries, encyclopaedias, etc.
- Researching and learning through the school's network
- Ensuring your device is fully charged before bringing it to school
- Being courteous, considerate and respectful of others when using your laptop. (e.g. sound)
- Switching off and placing your laptop out of sight when it is not being used.
- Seeking classroom teacher's approval when you want to use your laptop under special circumstances.

The following are examples of unacceptable use of devices by students:

- Using the device while on school grounds before or after school, or during lunch breaks.
- Using the device in an unlawful manner.
- Using the your school's email address to communicate with other students about matters not relating to school work.
- Creating, participating in or circulating content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place.
- Disabling settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard.
- Downloading (or using unauthorised software for), distributing or publishing of offensive messages or pictures.
- Using obscene, inflammatory, racist, discriminatory or derogatory language
- Using language and/or threats of violence that may amount to bullying and/or harassment.
- Deliberately wasting printing and internet resources.
- Intentionally damaging devices, accessories, peripherals, printers or network equipment.
- Intentionally committing plagiarism or violating copyright laws.
- Using unsupervised internet communication tools.
- Sending chain letters or spam email (junk mail).
- Accessing private internet networks during school hours or whilst at school.
- Knowingly downloading viruses or any other programs capable of breaching the Department of Education's network security.
- Using the laptop's camera without a classroom teacher's permission.
- Invading someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material
- Using the laptop (including those with Bluetooth functionality) to cheat during tests or assessments.
- Using the laptop's camera to record, photograph or film any students or school staff without the permission of the individual/s concerned and the supervising staff member.
- Copying files or passwords belonging to another user without their permission may constitute plagiarism and/or theft.

- Parents and caregivers need to be aware that intentional damage to laptops owned by other students or staff may result in consequences in relation to breaches of expectations and guidelines in the school's Student Code of Conduct.

The school's BYOD program supports personally - owned laptops in terms of access to:

- printing
- internet
- file access and storage
- support to connect devices to the school network.

However, the school's BYOD program does not support personally-owned mobile devices in regard to:

- complex technical support
- charging of devices at school
- security, integrity, insurance and maintenance
- private network accounts.

Responsible use Agreement:

- I have read and understood the BYOD Agreement and the school's Student Code of Conduct.
- I agree to abide by the guidelines outlined in both documents.
- I am aware that non-compliance and/or inappropriate behaviour, as per the intent of the BYOD Agreement and the Student Code of Conduct, will result in consequences relative to the behaviour.

Appendix 1
Frequently Asked Questions

What if we are unable to participate in the program due to financial reasons?
The school will continue to provide shared laptops across Year 5 & 6 classes for students to use while they are at school. Families who are not in a position to purchase a laptop are asked to make contact with the Deputy Principal to discuss alternative options.

I believe that Year 5 & 6 children are too young to have the responsibility for looking after a personal laptop. How will the school educate the children about how to safety use and transport their laptop?
As part of the Australian Curriculum ICT General Capability, students will be explicitly taught the expectations for how to care for a laptop and how to safely transport the device to and from school. Parents are encouraged to purchase a hard case for the laptop to protect it when it is in student bags. There are already a significant number of State Primary Schools running BYOD programs.

We are concerned about the security of laptops while they are at school. How will the school ensure that they are secured before school and during lunch breaks?
When students arrive to school, they will be encouraged to securely store their laptop in their classroom from 8:30am or in a locker. All laptops will be stored securely in classrooms during break times.

Our child is transitioning private high school and they provide a laptop as part of the tuition fees. What other options are there for my child to participate without having to purchase a new laptop?
The school will allow students in this position to bring their own device that they currently have at home that meets the school's minimum specifications. Parents can also make contact with the Deputy Principal to meet and discuss alternative options.

Will I need to bring the device to school every day?
Yes. Laptops are essential tools in each classroom.

How do I protect my BYOD device?
It is the student's responsibility to have their device with them at all times whilst in the classroom. Purchasing protective equipment such as bags or cases is recommended to keep these devices safe while at school, and travelling to and from school. It is the responsibility of the student to look after the device while at school and keep securely in bags.

We already have a device at home; can it be used at school?
Yes, if the device meets the minimum hardware and software minimum specifications.

Will every device work inside the Department of Education's network?
No. Some devices with low specifications have been found to not connect to the network. These devices may have difficulty with the security filters used by the Department of Education.
Will the school assist me with network connection settings at school?

Yes. Students will be provided with support from our IT Team and to connect to the school's network.

Will the school protect the device from virus attacks?
Virus protection remains the responsibility of the parent.

Does the school provide software for my BYOD device?
The Microsoft Office Suite is available free of charge for five student downloads at home. This will need to be downloaded to your child's laptop at the beginning of the school year.

Can get my BYOD device repaired at school?
Unfortunately all repairs will have to be sourced outside of school. Our IT team cannot perform software or hardware repairs on privately owned devices.

Will the school assist me with home internet connection settings and issues?
No. Your home internet provider or local computer technician can assist you with these enquiries.

Will the teacher be able to provide technical support in class?
No. Our IT support team is available for students before and after school and during break times to assist students with technical issues.

Can I bring my charger to school?
No. It is the student's responsibility to attend school every day with a fully charged laptop.

What is the school's view on an acceptable amount of screen time per day?
We have conducted research through the Australian Health eSafety Institute into recommended screen time for children and we want to reassure you that our curriculum delivery methods that require students to use their laptop will be under the time limits that this research suggests is reasonable.

Appendix 2
ICT User Agreement *(reviewed and agreed to during enrolment)*

Information and Communications Technology (ICT) User Agreement

Guidelines for ICT use at Buderim Mountain State School

Information and Communications Technology (ICT) facilities and devices provide innovative and engaging opportunities for teaching and learning. ICT is provided at Buderim Mountain State School for educational and research purposes. **This User Agreement sets out the expectations for acceptable use of ICT for all students.**

This agreement must be read in conjunction with the Department of Education, Training and Employment (DETE) policies relating to Acceptable use of ICT and Managing Electronic Identities (http://ppr.det.qld.gov.au/corp/ict/management/Pages/Acceptable-Use-of-Departments-Information-Communication-and-Technology-(ICT)-Network-and-Systems.aspx

http://ppr.det.qld.gov.au/corp/ict/management/Pages/Managing-Electronic-Identities-and-Identity-Management.aspx). Where terms used in this document have a definition under those policies those definitions apply to this agreement.

Every new student at Buderim Mountain State School is provided with a copy of this ICT User agreement for review, discussion and signing with their parent/caregiver at time of enrolment or if changes have been made or this documented is updated. **This user agreement will remain in effect for the duration of the student's enrolment at Buderim Mountain state School.** In the event that any amendments or additions are required to be made to this agreement, you will be advised in writing.

Buderim Mountain State School is committed to promoting and maintaining a culture of online behaviour that provides a safe, respectful and disciplined environment for students and staff. With the support of DETE, Buderim Mountain state School employs systems to assist in managing and monitoring student access to ICT and avoiding and reducing access to harmful online content and materials.

While every reasonable effort is made by the school to ensure students' use of ICT is safe and positive, developing positive online behaviours and protecting against negative influence is an ongoing and collaborative task that requires the active involvement of parents and caregivers. **It is encouraged and expected that parents and caregivers will discuss this user agreement with their child.**

Online behaviours can impact upon students' right to learn, teachers' ability to teach and the ability of the school to provide a safe, supportive learning environment. **Where inappropriate online behaviours negatively affect the good order and management of the school, the school may commence disciplinary actions in line with this user agreement or the Responsible Behaviour Management Plan.**

Buderim Mountain State School invites parents and caregivers to contact school staff to discuss any questions about cybersafety or this user agreement.

Principles of Acceptable Use of the ICT agreement at Buderim Mountain State School

For the purpose of this document 'I' refers to the student. For students entering prep, years 1,2,3. The parent / carer may sign on their behalf.

1. I will use only my designated personal account to access the school ICT and network. I will protect my account information, including username and passwords, and will not share this information with any other person.

2. If I become aware that another student's account details are being shared, I will advise a teacher or responsible staff member as soon as possible.

3. I understand that my online behaviours are capable of impacting on the good order and management of the school whether I am using the school's ICT inside or outside of school hours. I understand that my online behaviour should comply with this user agreement at all times.

4. If I find any online content that is offensive, abusive or that I know is against the school's Responsible Behaviour Management Plan, I will report this to a teacher as soon as possible. I will not save copy or distribute any offensive or inappropriate material content to any other person.

5. Online behaviours require the same attention to etiquette, courtesy and accountability as any other behaviour. I understand that online behaviours and content are capable of being shared online and reposted to a large audience.

6. **The use of ICT is a privilege and misuse may result in my access being restricted, suspended or subject to increased monitoring and supervision**.

7. **Despite departmental systems to manage access to information on the Internet, illegal, dangerous or offensive content may be accessed or accidentally displayed**.

8. I understand that school staff, with the support of the Department, will always exercise their duty of care, but avoiding or reducing access to harmful content also requires that I am responsible in my use of the ICT network and obey acceptable use policies and teacher directions.

9. I understand that the school and the Department monitor access to and usage of the ICT network. For example, e-mail monitoring will occur to identify inappropriate use, protect system security, maintain system performance, determine compliance with State and departmental policy and determine compliance with State and Federal legislation and regulation.

10. **Online behaviour can form the basis for criminal offences. The school may need to report serious instances of inappropriate online behaviour or content to police**.

11. Behaviour that is in violation of this acceptable use agreement may form the basis for the school to take disciplinary action against me.

12. **Buderim Mountain State School restricts the use of personal ICT devices on school grounds**. Personal ICT devices are used at their owners' risk. **No liability will be accepted by the school or Department in the event of loss, theft or damage to any device unless it can be established that the loss, theft or damage resulted from the Department's negligence.**

13. In the event that the use of a personal ICT device is required for educational purposes, it is the responsibility of the student, with their parent/caregiver, to negotiate with the school for special permission to use the private ICT device during school hours and/or on the school network.

Appendix 3
Private Feeder High School Information

At Buderim Mountain State School, our Year 6 students traditionally transition to a wide range of state and private high schools across the Sunshine Coast. We have listed the requirements for our feeder secondary private schools below to assist parents in making decisions about which device to purchase/use.

- Matthew Flinders - devices provided by the school as part of tuition fees
- Immanuel Lutheran College - devices provided by the school as part of tuition fees
- St Johns – devices provided by the school as part of tuition fees
- Nambour Christian College – devices provided by the school as part of tuition fees
- Suncoast Christian College - devices provided by the school as part of tuition fees
- Sunshine Coast Grammar School – BYOD (see specification requirements below)
- Siena Catholic College - devices provided by the school as part of tuition fees
- Pacific Lutheran College - BYOD (see specification requirements below)

Minimum Specifications	**Sunshine Coast Grammar School**	**Pacific Lutheran College**
Operating System	Windows 10	Windows 10
Processor	Intel i5 Processor	Intel i5 Processor
CPU Max Speed	Not stated	Not stated
Memory (RAM)	8GB	8GB
Storage Capacity (Hard Drive)	256 GB SSD	256 GB SSD
Screen Size	Not stated	11”
Graphics	Not stated	Not stated
Wireless Connectivity	Intel or Broadcom 802.11ac or better (No Atheros wireless chips)	Not stated
Battery Life	6 hours	Not stated
Speakers	Not stated	Not stated
Ports	Not stated	Not stated
Suggested Accessories	Protective case/cover Headphones Mouse Full size physical keyboard Touch Pad	Full size physical keyboard Touch Pad