



Dalby State High School

Student Laptop Charter Agreement

Nicholson Campus

Nicholson Street, DALBY QLD 4405
Postal: PO Box 608, DALBY QLD 4405
T (07) 4669 0900
E admin@dalbyshs.eq.edu.au

Bunya Campus

463 Bunya Highway, DALBY QLD 4405
Postal: 463 Bunya Highway, DALBY QLD 4405
T (07) 4660 0333
E admin@dalbyshsbunya.eq.edu.au

Contents

Personally—owned laptop charter	3
BYOL overview	3
Laptop Specifications	4
Laptop care	5
Data security and back-ups	5
Acceptable personal laptop use	6
Passwords	6
Digital citizenship	7
Cybersafety	7
Web filtering	8
Privacy and confidentiality	8
Intellectual property and copyright	8
Software	9
Monitoring and reporting	9
Misuse and breaches of acceptable usage	9
Responsible use of laptops	10
Frequently Asked Questions	13
Fact sheets for Parents and Carers	16
Property Identification	18
BYOL agreement (to be signed & returned)	19

Personally-owned laptop charter

BYOL overview

Bring Your Own 'Laptop' (BYOL) is the pathway supporting the delivery of 21st century learning. It is a term used to describe a digital device ownership model where students or staff use their personally-owned mobile devices to access the department's information and communication (ICT) network.

At Dalby SHS these mobile devices are limited to laptops. Access to the department's ICT network is provided only if the laptop meets the department's security requirements which, at a minimum, requires that anti-virus software has been installed, is running and is kept updated on the device [Advice for State Schools on Acceptable use of ICT Facilities and Devices](#).

Students and staff are responsible for the security, integrity, insurance and maintenance of their personal laptops and their private network accounts.

The BYOL acronym used by the department refers to the teaching and learning environment in Queensland state schools where personally-owned laptop devices are used. The 'L' in BYOL represents more than a personally-owned laptop device; it also includes software, applications, connectivity or carriage service.

We support the implementation of a BYOL model because:

- BYOL recognises the demand for seamless movement between school, work, home and play
- our BYOL program assists students to improve their learning outcomes in a contemporary educational setting
- assisting students to become responsible digital citizens enhances the teaching learning process and achievement of student outcomes as well as the skills and experiences that will prepare them for their future studies and careers.

Laptop Specifications

Before acquiring a laptop to use at school, the parent/carer and student should be aware of the school's specification of the laptop's operating system requirements and software. These specifications relate to the suitability of the laptop to enabling class activities, meeting student needs, and promoting safe and secure access to the department's network.

Dalby State High School's BYOL program may support printing, filtered internet access and file access and storage through the department's network while at school. However, Dalby State High School's BYOL program does not include school technical support or charging of devices at school.

The table below outlines of what the current and suitable standard for a BYO device:

Specification	Minimum	Recommended	Performance
Processor (CPU) ¹	Intel i3 10 th Gen and above	Intel i5 10 th Gen and above	Intel i7 10 th Gen and above
Memory (RAM)	8 GB	16 GB	16 GB
Wireless	Wi-Fi 5 (802.11ac)	Wi-Fi 6 (802.11ax)	Wi-Fi 6 (802.11ax)
Storage ²	256 GB SSD	256 GB SSD	512 GB SSD
Operating System ³	Windows 11 Home (22H2 or newer version)		
Warranty ⁴	Preferably 3 years warranty		
Display ⁵	Size: 12" Display Min. Resolution: 1366 x 768	Size: 14" Display Min. Resolution: 1600 x 900	Size: 15" Display Min. Resolution: 1920 x 1080
External Ports	At least 1 USB 2.0, 1 USB 3.0 and 3.5mm headphone jack		

¹ AMD Ryzen CPU equivalent

² SSD stands for Solid-State Drive

³ Windows S Mode **will not** work. Update your OS to full version!

⁴ By default, manufacturer warranty is 1 year. Accidental Damage cover is highly recommended.

⁵ Display will factor a number of things like Aspect Ratio, Refresh Rate, Screen Definition, and so. Follow the recommended setting.

Additional Notes

- Apple products (MacBook, MacBook Air, MacBook Pro) **are** compatible with our BYOL program for **internet access only**. Printing, network drives, and other services **are not** operational
- iOS (iPhone, iPods or iPads) and Android devices **are not** supported by the school. Please see the Electronic Device Policy
- All ARM based devices are **not** supported by the department as of 01/12/2025 but support is underway with no specified date yet
- Regardless of what the student will do with their device throughout the day, the battery settings must be configured and **the battery must hold for at least 6 hours**
- By default, any Windows based OS will have a Microsoft Defender for anti-virus protection. Please install your preferred software to protect your data and device. AVAST and some other anti-virus software **are not** compatible
- Windows OS and all Microsoft application must be **fully updated** prior to device enrolment
- Any parental control service installed on the device might cause an issue with the school's network proxy. Please consider enabling proxies for internet access
- DSHS P&C Association have a locker system in place for safe storage of student property. See Resources Centre
- As at Nov 2025, while this general specification table is compatible with our school network. Please be aware that specific make and model of components or combinations thereof can still cause issues with network connections and/or operations.

Laptop care

The student is responsible for taking care of and securing the laptop and accessories in accordance with school policy and guidelines. Responsibility for loss or damage of a laptop at home, in transit or at school belongs to the student. Advice should be sought regarding inclusion in home and contents insurance policy.

It is advised that accidental damage and warranty policies are discussed at point of purchase to minimise financial impact and disruption to learning should a laptop not be operational.

General precautions

- Food or drink should never be placed near the laptop.
- Plugs, cords and cables should be inserted and removed carefully.
- Laptops should be carried within their protective case where appropriate.
- Carrying laptops with the screen open should be avoided.
- Ensure the battery is fully charged each day.
- Turn the laptop 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 laptop 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.

Data security and back-ups

Students must ensure they have a process of backing up data securely. Otherwise, should a hardware or software fault occur, assignments and the products of other class activities may be lost.

The student is responsible for the backup of all data. While at school, students may be able to save data to the school's network, which is safeguarded by a scheduled backup solution. All files must be scanned using appropriate anti-virus software before being downloaded to the department's ICT network.

Students are also able to save data locally on their laptop 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 an external hard drive or USB drive.

Students should also be aware that, in the event that any repairs need to be carried out the service agents may not guarantee the security or retention of the data. For example, the contents of the laptop may be deleted and the storage media reformatted.

Acceptable personal laptop 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](#)

This policy also forms part of this Student Laptop Charter. 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 department's Code of School Behaviour and the Student Code of Conduct available on the school website.

While on the school network, students should not:

- create, participate in or circulate content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disable settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
- use unauthorised programs and intentionally download unauthorised software, graphics or music
- intentionally damage or disable computers, computer systems, school or government networks
- use a device for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

Note: Students' use of internet and online communication services may be audited at the request of appropriate authorities for investigative purposes surrounding inappropriate use.

Passwords

Use of Dalby SHS's ICT network is secured with a user name 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 divulged to other individuals (e.g. a student should not share their username and password with fellow students).

The password should be changed regularly, as well as when prompted by the department or when known by another user.

Personal accounts are not to be shared. Students should not allow others to use their personal account for any reason.

Students should log off at the end of each session to ensure no one else can use their account or laptop.

Students should also set a password for access to their BYOL device and keep it private.

Parents/caregivers may also choose to maintain a password on a personally-owned laptop for access to the device in the event their student forgets their password or if access is required for technical support. Some devices may support the use of parental controls with such use being the responsibility of the parent/caregiver.

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 have 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 a class or the broader community.

Parents are requested to ensure that their child understands this responsibility and expectation. Dalby SHS's Student Code of Conduct also supports students by providing school related expectations, guidelines and consequences.

Cybersafety

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 inform their teacher, parent or caregiver as soon as is possible.

Students must also seek advice if another user seeks personal information, asks to be telephoned, offers gifts by email or asks to meet a student.

Students are encouraged to explore and use the [‘Cybersafety Help button’](#) to talk, report and learn about a range of cybersafety 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 the *Student Code of Conduct* and any specific rules of the school. To help protect students (and staff) from malicious web activity and inappropriate websites, Dalby SHS 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 staff and 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. Any suspected security breach involving students, users from other schools, or from outside the Queensland DET network must also be reported to the school.

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/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 or for reasons other than to fulfil the educational program requirements of the school. 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. 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.

Intellectual property and 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 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.

Copying of software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.

Software

Schools may recommend software applications in order to meet the curriculum needs of particular subjects. Parents/caregivers may be required to install and support the appropriate use of the software in accordance with guidelines provided by the school. This includes the understanding that software may need to be removed from the laptop upon the cancellation of student enrolment, transfer or graduation.

Monitoring and reporting

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 laptop 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.

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.

Dalby SHS reserves the right to restrict/remove access of personally owned laptops 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 laptops may result in disciplinary action which includes, but is not limited to, the withdrawal of access to school supplied services and/or submission of device to office as per Electronic Device Policy.

Responsible use of Laptops

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 BYOL program:

School

- network connection at school
- internet filtering (when connected via the school's computer network)
- some technical support (please consult Technical support table below)
- some school-supplied software e.g. Adobe, Microsoft Office 365 ...
- printing facilities
- school representative signing of BYOL Charter Agreement.

Student

- acknowledgement that core purpose of laptop 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 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)
- some technical support (please consult Technical support table below)
- maintaining a current back-up of data
- charging of laptop
- abiding by intellectual property and copyright laws (including software/media piracy)
- internet filtering (when not connected to the school's network)
- ensuring personal login account will not be shared with another student, and laptop will not be shared with another student for any reason
- understanding and signing the BYOL Charter Agreement.

Parents and caregivers

- acknowledgement that core purpose of laptop 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 (please consult Technical support table below)
- required software, including sufficient anti-virus software
- protective backpack or case for the laptop
- adequate warranty and insurance of the laptop
- understanding and signing the BYOL Charter Agreement.

Technical support

	Connection:	Hardware:	Software:
Parents and Caregivers	✓ (home-provided internet connection)	✓	✓
Students	✓	✓	✓
School	✓ school provided internet connection	(dependent on school-based hardware arrangements)	✓ (some school-based software arrangements)
Device vendor		✓ (see specifics of warranty on purchase)	

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

- Use laptops for:
 - engagement in class work and assignments set by teachers
 - developing appropriate 21st Century 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, teachers, parents, caregivers or experts as part of assigned school work
 - accessing online references such as dictionaries, encyclopaedias, etc.
 - researching and learning through the school's eLearning environment
 - ensuring the device is fully charged before bringing it to school to enable continuity of learning.
- Be courteous, considerate and respectful of others when using a mobile device.
- Switch off and place out of sight the mobile device during classes, where these laptops are not being used in a teacher directed activity to enhance learning.
- Use the personal mobile device for private use before or after school, or during recess and lunch breaks.
- Seek teacher's approval where they wish to use a laptop under special circumstances.

The following are examples of irresponsible use of laptops by students:

- using the laptop in an unlawful manner
- 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, or even stalking
- insulting, harassing or attacking others or using obscene or abusive language
- deliberately wasting printing and Internet resources
- intentionally damaging any devices, accessories, peripherals, printers or network equipment
- committing plagiarism or violate copyright laws
- using unsupervised internet chat

- sending chain letters or spam email (junk mail)
- accessing private 3G/4G networks during lesson time
- knowingly downloading viruses or any other programs capable of breaching the department's network security
- using the mobile device's camera anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets
- 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 mobile device (including those with Bluetooth functionality) to cheat during exams or assessments
- take into or use mobile devices at exams or during class assessment unless expressly permitted by school staff.

In addition to this:

Information sent from our school network contributes to the community perception of the Dalby SHS. All students using our ICT facilities are encouraged to conduct themselves as positive ambassadors for Dalby SHS.

- Students using the system must not at any time attempt to access other computer systems, accounts or unauthorised network drives or files or to access other people's laptops without their permission and without them present.
- Students must not record, photograph or film any students or school personnel without the express permission of the individual/s concerned and the supervising teacher.
- Students must get permission before copying files from another user. Copying files or passwords belonging to another user without their express permission may constitute plagiarism and/or theft.
- Students need to understand copying of software, information, graphics, or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.
- Parents and caregivers need to be aware that damage to laptops owned by other students or staff may result in significant consequences in relation to breaches of expectations and guidelines in Dalby SHS's Student Code of Conduct.
- The school will educate students on cyber bullying, safe internet and email practices and health and safety regarding the physical use of electronic devices. Students have a responsibility to incorporate these safe practices in their daily behaviour at school.

Dalby SHS's BYOL 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 BYOL program does not support personally-owned laptops in regard to:

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

BYOL FAQs

Q: What is BYOL?

A: BYOL stands for “Bring Your Own Laptop.” BYOL is an initiative that will allow students who have personal technology devices to bring them to school, to use them for educational purposes to meet their learning needs under the direction of a teacher.

Q: What are the benefits of BYOL?

A: Our students are living in a world where they have immediate access to information anytime and anywhere. Many students have personally-owned devices that can be used to allow them to learn in their own style and at their own pace. With digital learning, every student can access high quality and rigorous instruction, thereby maximising their opportunity for success in school and beyond.

Specific benefits include:

- Allowance for personalised learning
- Improved student learning outcomes
- Improved collaboration
- Give student greater choice and more independence
- It creates a model for lifelong learning
- Smooth transition between home and school
- Allows 24/7/365 access
- Provides easier student access to online instructional materials
- Supplements school resources and equipment
- Normalisation of technology

Q: Why only allow laptops?

A: We believe in a consistent approach to ensure best productivity with regards to maximising student learning outcomes.

Q: Which year levels can BYOL at Dalby SHS?

A: All students are welcome to bring their own laptop to school to supplement their educational requirements. This may be to research and prepare assignments. Year 7 and 8 students who BYOL will have dedicated IT-based pedagogical practices.

Q: Will I be expected to purchase a new laptop and do I have to purchase from a particular store e.g. Dell, HP?

A: No, you can choose to use a laptop that you already own or purchase a new laptop but it must meet the minimum specifications required by the school. No, we will not recommend a store where you can purchase a laptop; however, we can provide details of providers. We do not endorse any one store.

Q: Should we purchase a carry case for the laptop and if so, which one should we buy?

A: Yes, you should purchase a carry case. We recommend that the carry case should protect both the front and back of the laptop. We will not recommend a store where you can purchase a case or cover. We do not endorse any one store.

Q: Will Year 7 students use their laptop in every session of everyday?

A: This is unlikely due to the practical nature of some year 7 electives (ie Home Economics and/or Performing Arts).

Q: Can my child bring a 3G enabled laptop without the SIM?

A: Yes. The reason why we do not want external controlled Internet access is that by the students going through our school wireless, they are also going through Education Queensland Internet filters, helping protect our students from accessing inappropriate content.

Q: Are we required to purchase a stylus pen?

A: Yes, if you purchase a laptop with touch screen possibilities.

Q: Will my child require a username and password?

A: Yes. It is a departmental requirement that a username and password is used to access the school network. This is provided by the school.

Q: My child has a laptop at home already. Will that laptop be suitable for use at school?

A: Any laptop that meets the minimum specifications for the BYOL program is suitable for use at school.

Q: Where can I purchase a suitable laptop?

A: Laptops can be purchased from a range of retailers.

Q: What happens if a student uses a laptop inappropriately?

A: The Electronic Devices Policy will outline the sanctions for inappropriate use of laptops and network. Students and their parents will be required to sign agreements that these policies will be adhered to and that consequences of policy breaches are understood before network access is provided.

Q: What about security, theft and damage to the laptop?

A: Laptops will be the responsibility of the student. During class time students will be able to bring their laptop into class, unless it is not practical to do so (ie HPE prac). Laptops will need to be stored in bags at break times. Students can opt to get a locker to secure items whilst at school, hire available through Textbook Hire.

Parents are advised to review their insurance policies to ensure that BYOL is covered outside the home, and to provide a suitable protective bag for the laptop. The school will accept no responsibility for the security or safety of the laptop.

Q: Do I need a warranty?

A: We strongly recommend that all laptops have some form of extended warranty. While research shows that students take much better care of a laptop which belongs to them than a school provided laptop, accidents happen.

Q: What is the policy for charging personally owned laptops while at school?

A: It is expected that personally owned laptops are brought into school with a full charge. Students will be made aware that the school is not responsible to provide an opportunity or the necessary power to charge their laptop during the school day.

Q: What is the policy for printing from personally owned laptops?

A: Students will be able to access printing at school.

Q: How much of the time will students be using their own laptop?

A: Teachers will direct students to use laptops where they are the best tool for learning. This will vary between year groups and subjects studies.

Q: What is “Intune Device Enrolment”?

A: *Intune Device Enrolment is the technical term used to describe the procedure that students need to perform to get their laptops operational on the school network. Dalby State High School uses a system that allows safe, secure, and largely automatic on-boarding for most laptops, and information about the use of this system will be provided to students when they join the BYOL program. Students will require administrative access to complete the Intune Device Enrolment process. If students require any assistance with Intune Device Enrolment of their laptop, they are free to contact the school's ICT Support.*

Q: Will the school assist me with home internet connection settings, or issues?

A: *This is not part of the support offered by the school. The school's support is limited to providing assistance with Intune Device Enrolment of the laptop to the network and curriculum related inquiries. If you require assistance for personal issues regarding your laptop, your home internet service provider or private computer technician should be able to assist with these enquiries.*

Q: Do students need to backup the data stored on their laptop?

A: *Backup of laptop data is the student's responsibility. Work that is completed at school can be saved to the school's servers. However, work completed at home or stored on the laptop will need to be backed up in case the laptop encounters a problem such as a hardware failure.*

Q: How will students be kept safe online?

A: *Access to the Internet at school is filtered. As part of the curriculum, students are instructed on Cyber safety. At home, it is the parent/guardian's responsibility to ensure any appropriate content filters or controls are applied to internet services. The school accepts no responsibility for consequences of internet access outside the school.*

Q: What should I consider if I am purchasing a new laptop?

- *Specifications – minimum specifications are provided in this booklet and on the school website*
- *Life of the device – consider the length of time you require the device to service the needs of your family*
- *Add-ons – beware of adding unnecessary additional features as this will increase the price of the device*
- *Length of warranty – extending the warranty to 3-4 years is advisable*
- *Warranty conditions – consider what the warranty covers (read the fine print)*
- *Personal contents insurance – determine if this covers laptop/digital device damage away from the home (accidental damage)*
- *Cost of repairs – screen and keyboard are the most commonly damaged parts*

Q: Who can I contact for further information?

A: *Please contact the school office on 4669 0900 or admin@dalbyshs.eq.edu.au for further information.*

Fact Sheet for Parents and Carers

BYOxLink Getting your child's device ready for school

The Department of Education is implementing a new Bring Your Own (BYO) device solution called "BYOxLink" that enables students to use their privately owned devices to access school email, learning applications, printers and shared network drives at the school.

As part of the BYOxLink project rollout, schools wireless systems will be updated to handle access from private devices and Microsoft Intune; a mobile device management platform, will also be introduced.

What does "enrolling your child's device into Intune", mean for my child?

Enrolling your child's device into Intune, will mean your child will be able to:

- access the school Wi-Fi network and have school email automatically set up and configured
- access the school's learning applications and websites
- self-manage their personal device

What if I am having trouble with the enrolment?

If you are having trouble or have further questions, contact your school IT support or school administration staff.

Please note, your child will need to stay logged in for up to 15 minutes after enrolment is done, to make sure all Intune set-up is complete. Enrolment of a device may take 10-15 minutes.

Where is it best to enrol my child's device into Intune?

We recommend that your child enrolls their device into Intune at home using the home Wi-Fi internet connection. If needed, your child may also enrol at school, using the school guest Wi-Fi service, EQGUEST.

How much home internet data allowance does Intune use?

A small amount of data is required to both enrol your child's device into Intune and subsequently to use Intune at home to access school email and learning applications. Home data allowance will be required if your child is accessing websites and school applications; the amount depends on the applications.

What the school administration (Intune) can see or not see on my child's device?

What the school administration (Intune) can see on the device	What the school administration (Intune) cannot see on the device
<p><i>Your school can only see information that is relevant to the school:</i></p> <ol style="list-style-type: none"> a. Device owner. b. Device name. c. Device model. d. Device manufacturer. e. Operating system and version eg: Windows 10. f. App inventory and App names, like Microsoft Office 365. g. On student and staff's personal devices the school can only see school managed Apps. h. Device serial number and IMEI. 	<p><i>Your school does not monitor student's use of the device</i></p> <ol style="list-style-type: none"> a. Cannot see your child's personal information. b. Cannot see what your child is doing on their device. c. Does not track student's locations /device location. d. Does not provide information on personally installed applications. e. Does not allow uninstalling of any applications including your child's own applications. f. Home Network cannot be seen. g. Calling and web browsing history. h. Email and text messages. i. Contacts. j. Calendars. k. Passwords. l. Pictures, including what's in the photos app or camera roll. m. Files.

Can I have multiple mobile device management tools on my child's device?

Microsoft Intune does not work if other mobile device management (MDM) tools are installed on the device.

Can I use parental controls if my child's device has Intune installed?

Parental controls can be used in conjunction with Intune. Windows has Microsoft Family to manage screen time and block and manage apps and features on your child's device.

Is there any cost associated with using Intune?

There is no cost for your child to use Intune and Microsoft Office 365. Your child's school may impose charges for other application licensing costs.

What are the requirements for my child's device?

Your child's device needs to be supported by the manufacturer. See links below for the manufacturer lists of obsolete and discontinued products.

- *For windows devices, refer to Microsoft's category of discontinued products.*
- *For Apple and Mac devices, refer to statement of vintage and obsolete products. Note for Apple, that only Mac devices are supported by the BYOLink service offering.*

Update the operating system on your child's device to latest available operating system. Windows 11 22H2 or newer, MacOS 26 operating systems are compatible with the BYOLink service offering.

Property Identification

Marking your property makes ownership clear and deters theft as marked property is more difficult for the thief to offload. Marked property also helps police to identify and return it to the rightful owner.

Property that is most at risk of being stolen is desirable, usually small, has a good re-sale value and is able to be off loaded and sold quickly. Typically, this includes computers, cameras, multi-media devices, satellite navigation devices, mobile phones, power tools and bicycles.

Follow these steps to mark your property:

STEP 1:

Mark your property by engraving or microdoting them. Where possible, mark your property with a code on the top right hand rear corner of the item or near to the manufactures serial number. Take a video or photograph of property that can't be marked, such as jewellery.

STEP 2:

After marking your property, visit your local police station, Police Beat shopfront or neighbourhood Police Beat and tell them your code. You can also collect ID warning stickers to place on your engraved items and on your doors or windows to act as a deterrent to would-be intruders.

STEP 3:

Keep accurate records. Write an inventory as this will help you make an insurance claim and assist police recover stolen items. List the serial, make and model numbers and keep the original receipts of valuable items and store this information along with any valuation certificates in a safe place.

Engraving

Engravers are available for loan from your local police station, Police Beat shopfront, neighbourhood police beat or Neighbourhood Watch Area Coordinator (at no cost). You should seek operating advice before using an engraver as not all items are suitable for engraving.

Property identification involves marking your property with a personal code. The Queensland Police Service recommends you create a personal code.

A personal code is created by using details such as the first initial of your first name, the first initial of your surname, date of birth and State of residence. For example, the personal code for

Cameron Peters,

Born on 1 August 1974, would be: **CP 010874 Q**

Dalby State High School

Bring Your Own Laptop (BYOL) Agreement

This form is required to be signed and returned to the school office.

The following program can also be added on if required:

☐ I require the additional Adobe package for specialist subjects eg Design

The student and parent/caregiver are required to carefully read this agreement before signing it. Any questions should be addressed to our Network Administrator, Dinesh Lee (Ph. 4669 0900) and clarification obtained before the agreement is signed.

In signing below, I acknowledge that I:

- understand and accept all policies, conditions and guidelines as per the School's BYOL Student Charter Agreement; Student Code of Conduct for Students; Electronic Device Policy; Internet Access Agreement and BYOLink Parent/Carer Fact Sheet.
- accept responsibility for damage that may occur to the device within the School and have insured the device in case of damage or have chosen to self-insure the device
- understand that, should my device not meet minimum specifications as outlined in the BYOL Student Charter Agreement booklet, I may not be able to connect to the BYOL network at Dalby SHS

Student name:

Current Year Level:

Student signature:

Date: / /

Parent /caregiver name:.....

Parent /caregiver signature:

Date: / /