# BUNDAMBA STATE SECONDARY COLLEGE

PRIDE » RESPECT » RESPONSIBILITY » EMPOWERMENT

# BYOx Parent Charter

*Version 1.1, 2025*



Queensland Government

# Contents

# BYOx Overview

The way in which we learn, access, share and manage information is changing rapidly. There is an increasing need for students to access external learning content, collaborate with others in their educational pathway, and be proficient with the use of computer technologies. As a school we have a responsibility to prepare our young people for the future world that they enter.

We at Bundamba State Secondary College understand that the use of technology is more than just a method of searching for information; technology is a tool that enhances teaching and learning experiences, empowers the creation and sharing of knowledge, and allows students to learn at their own pace.

## What is the BYOx Program?

Bring Your Own 'x' (BYOx) is a new pathway supporting the delivery of 21st century learning, where 'x' extends beyond the physical device to include the necessary software, applications, and connectivity. The program will enable students to connect their personal devices to the school-provided BYOx link, granting access and connectivity to educational resources at school and home.

## What is the BYOx Link?

The BYOx Link is the technical service provided by the Department of Education. Providing more than just Wi-Fi, this service allows students to securely access our IT network, school email, school printers and online applications on their privately owned devices. To connect to BYOx Link personal devices must be enrolled via the company portal (Intune) application.

School staff can only access **school** information through Intune and **cannot**:

- see personal information
- monitor what happens on the device
- track or locate the device
- see information on installed personal applications (other than school applications)
- uninstall applications, including personal ones

## BYOx in Bundamba State Secondary College

From 2026, all students in years 7, 10, 11 and 12 will be required to bring an enrolled personal device to participate in the BYOx program.

We have chosen to support the implementation of the BYOx program to:

- allow seamless access to class resources between school and home
- increase access to learning tools
- promote independence and self-initiated learning
- boost engagement and student learning outcomes in a contemporary educational setting
- assist our students in learning how to use technology responsibly and ethically, fostering digital literacy through regular practical application
- prepare our learners for their future studies and careers by engaging in an organizational digital landscape

*Note: Students in other year levels may bring a device to support their learning once their caregiver has signed the BYOx Student Charter.*

## Device Specifications

To ensure consistent and reliable access our school network, printers, and software, it is *imperative* that your chosen personal device meet the minimum specifications outlined below. These requirements are **not** optional; **we cannot guarantee access if the minimum specifications are not met.**

Personal devices may be sourced from anywhere, provided they meet the requirements below:

| | |
|---|---|
| *Type | Microsoft Windows laptops or Mac Devices<br>**NOT Supported**: Mobile phones of any kind, iPads or tablets, and Chromebooks. |
| Screen Size | 11”-15” display – consider portability and weight |
| Processor | Intel Core i3 or above, Ryzen 3 or above |
| RAM | 8 GB or higher |
| Hard Drive | 128 GB Solid State Hard Drive (note: we recommend a solid-state hard drive (SSD) for performance)<br><br>Older style Hard Drives do not offer the same performance and are more likely to fail when moved around. However, if this is your only option, a minimum 128GB would be best. |
| *Operating System | Microsoft Windows 11 or MacOS 13 and above<br><br>Note: Windows 10 will be end of life by October 2025. If you are buying second-hand, please ensure your device can update to the latest version of windows.<br><br>**NOT Supported**: Android, IOS, Windows RT, ChromeOS and distributions of Linux |
| *Wireless Adapter | Wi-Fi 802.11ac/n or (**Wireless Network 5Ghz**). Look for the term “Dual Band”.<br><br>If the adapter is labelled “Single Band” please ensure it is the **Wireless Network 5Ghz** radio band. |
| Battery | Sufficient to last 6+ hours on balance power mode |

***Please note: Failure to meet the above requirements, especially where marked with an *, will result in the purchase of a device unable to be enrolled and not functional for school use.***

## Purchasing

To support our school community, we have engaged with various vendors to provide purchase portals for BYOx families. These purchase portals offer a 'one-stop-shop' for buying personal devices, relevant accessories and their respective warranty. All purchasable devices displayed in these portals are tailored to meet our specifications. Additionally, each portal has various payment options to make purchasing more accessible.

We have no financial affiliation with these vendors, any purchases made through these portals will not be organized or managed by the school. Subsequently any accessories or warranty purchased will not be organized or managed through the school.

We take no responsibility for any private laptop purchasing and/or finance arrangements. All issues with purchases, warranty/repair, or technical issues must be taken up with the vendor/supplier.

The use of these portals is optional, we encourage parents/caregivers to explore options while utilizing our device specifications to find a device that suits your child's needs and your budget.

We ask that families consider the below when purchasing.

### New device purchasing considerations:

- Many vendors will offer 'ADP' or 'Accidental Damage protection', this is an additional cover to the manufacturer warranty that greatly reduces or in some cases negates the costs associated with repairing physical damage. We recommend this product for extra peace of mind.

### Second-hand purchasing considerations:

- Please consider the age of the device, the average laptop will provide roughly 3-4 years of use before hardware begins to fail.
- Please ensure the device has been factory reset before providing the device for student use.

### General purchasing considerations:

- We recommend a protective hard case to reduce the risk of a broken screen.
- Please consider a back-up storage device (USB or External Hard Drive) for data backup.
- Devices cannot be shared between parents or other children, only one organizational account can be enrolled at a time due to restrictions with intune.

## Preparing Your Device

Once you have your device and have finished the initial setup, whether that be factory resetting a second-hand device or setting up your device new out of the box – It is **essential** that your device is enrolled to connect to BYOx Link.

BYOx Link provides student access using school user identity-based tokens, these are installed on your child's device during enrollment via the Company Portal application. Attempting to connect to school services **without** enrolling is known to cause:

- Sign-in issues with Microsoft
- Inconsistent network connection
- Limits in accessing school resources – Nil access to printing, limited app access, etc.
- Reduced device security and limited filtering.

As such, if your device is not enrolled it will not be suitable for class use.

Device enrollment is the responsibility of the device owner, it is recommended that you or your child enrolls their device into Intune at home using a home Wi-Fi connection. Enrollment guides are available on our school website in both written and video form.

If you are experiencing difficulty with setting up or enrolling your device, you can reach out to our school I.T support byod@bundambassc.eq.edu.au for assistance.

### Software installation

- Microsoft Office 365

  All students have Office 365 licenses by default. Office 365 can be downloaded for free by visiting *office.com* and using their department user identification to login. Please visit our school website for step-by-step instructions.

- Apps through the company portal

  depending on what subjects your child has chosen or what year level they are enrolled in various apps may be available for install on the company portal. Please be sure to check the apps section in the company portal app

- NAPLAN

  For years 7 and 9, the NAPLAN LDB can be downloaded for installation on student-managed devices. Notice will be sent out in advance about installation as the application is year specific.

- Antivirus

  We recommend Microsoft's free built-in anti-virus protection Windows Defender, this program receives frequent live updates with Windows providing active protection to new threats.

  New Windows laptops almost always come with a free trial of an Antivirus program e.g. McAfee or Norton. However, once the trial expires the program becomes effectively useless as without updated virus definitions to deal with new malware your computer is no longer properly protected. Additionally, these 3rd-party antivirus programs may reduce the device's performance or prevent your student from accessing some resources.

## Device 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. 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 device not be operational.

Bundamba State Secondary College will not be responsible for any loss, theft or damage to the device or data stored on the device. In circumstances where a device is damaged by abuse or malicious act of another student, the school will apply consequences in accordance with the Bundamba State Secondary College Student Code of Conduct, however Bundamba State Secondary College is not liable for the reimbursement or replacement of the device.

### Device Charging

It is the responsibility of the student to bring their laptop to school fully charged every day. Failure to bring laptops fully charged each day will impact on student learning and their ability to participate in class activities.
Students will **not** be able to charge laptops during class time. This is primarily due to workplace health and safety issues (e.g. cables being a trip hazard, power cables not "tested and tagged"). However, if a student requires their laptop to be charged (e.g. if it's an older laptop that doesn't hold its charge) there will be a charging station in the library that students will be able to access before school and at break times to charge their laptops securely.

### Device Safety

#### At *School*

- Keep your laptop with you at all times – Do **not** leave it in your bag outside of classrooms
- Keep your laptop in a protective hard case at all times
- Consider engraving the device – this will help identify any lost devices

#### *In General*

- Food or drink should never be placed near the device
- Cords and cables should be inserted and removed carefully
- Devices should be carried within their 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
- Avoid poking at the screen — even a touch screen only requires a light touch
- Do not carry the device by the screen – carry it holding the base of the laptop
- Do not 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
- Do not clean the screen with a household cleaning product

## Data Backup

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. 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 to their 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 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 might not guarantee the security or retention of the data. For example, the contents of the device may be deleted, and the storage media reformatted.

Through Microsoft Office 365, students have access to OneDrive for Students. This is a cloud-based service that is linked to their Office 365 Suite and school log in details. It is recommended that all students back up their files in their OneDrive.

## Technical Support

Device enrollment, software installation, updating software/systems, and general device maintenance is the responsibility of the parent/caregiver or student; However if required, our IT team may be able to assist with the following:

- General IT advice and recommendations
- Inspecting for faults or issues
- General troubleshooting
- Installing or uninstalling software
- Wiping or factory resetting
- Reinstalling windows
- Device enrollment

Where possible, our IT team will always try to avoid factory resetting, reinstalling Windows, or uninstalling personal software. If these services are required, our staff will communicate any potential results or data loss to the student before completing works.

It is assumed the student will be following guidelines and is backing up their data appropriately. Our staff will not be responsible for any data loss as a result of maintenance or support.

If you do not wish to receive the above technical support you will need to provide, **in writing**, that you would like to opt out of our technical support service. This opt out notice can be handed into admin or emailed to byod@bundambassc.eq.edu.au

Support and assistance is subject to staff availability. General support will be limited If your device is not enrolled. Support will not be provided to devices that do not meet our specifications.

Physical device/hardware issues will be the responsibility of the parent/caregiver and student. All Physical device/hardware issues should be referred to the vendor/warranty. Vendor and technical support turnaround times should be considered when purchasing and seeking repairs for devices.

## Acceptable personal device 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 (located on our school website).

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 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 Wiping or factory resetting
- 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 the 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 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 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 also set a password for access to their BYOx 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 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. The school's Student Code of Conduct also supports students by providing school related expectations, guidelines and consequences.

## 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 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 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, available on our website.

## 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 from malicious web activity and inappropriate websites, the school 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.

BYOx 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. Parents, caregivers and students are also encouraged to visit the website of the Australian eSafety Commissioner for resources and practical advice to help young people safely enjoy the online world.

## 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 device 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 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.

## 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 school reserves the right to restrict/remove access of personally owned 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 devices may result in disciplinary action which includes, but is not limited to, the withdrawal of access to school supplied services.

## Responsible Use of BYOx

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 BYOx program

*School*

- BYOx program induction — including information on (but not responsible for) connection, care of device at school, workplace health and safety, appropriate digital citizenship and cybersafety
- 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 BYOx Charter Agreement.

*Student*

- participation in BYOx program induction, including device enrollment
- acknowledgement that core purpose of device at school is for educational purposes
- care of device
- appropriate digital citizenship and online safety (for more details, visit the website of the Australian eSafety Commissioner)
- 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
- maintaining a current back-up of data
- charging of device
- 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 device will not be shared with another student for any reason
- understanding and signing the BYOx Charter Agreement.

*Parents and caregivers*

- participation in BYOx program induction, including device enrollment
- 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 (for more details, visit the website of the Australian eSafety Commissioner)
- some technical support (please consult Technical support table below)
- required software, including sufficient anti-virus software
- protective backpack or case for the device
- adequate warranty and insurance of the device
- understanding and signing the BYOx Charter Agreement.

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

- Use of personal devices 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 schoolwork
    - 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 device.
- Switch off and place out of sight the device during classes, where these devices are not being used in a teacher directed activity to enhance learning.

## The following are examples of irresponsible use of devices by students:

- Using the device 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
- 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 device (including those with Bluetooth functionality) to cheat during exams or assessments

## In addition to this:

- Information sent from our school network contributes to the community perception of the school. All students using our ICT facilities are encouraged to conduct themselves as positive ambassadors for our school.
- 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 devices 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 devices owned by other students or staff may result in significant consequences in relation to breaches of expectations and guidelines in the school'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.

The school's BYOx program supports personally-owned devices in terms of access to:

- Printing
- Internet
- file access and storage
- support to connect devices to the school network.

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

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

## Responsible use agreement

The following is to be read and completed by both the STUDENT and PARENT/CAREGIVER:

I have read and understood the BYOx Charter and the school Student Code of Conduct.

I agree to abide by the guidelines outlined by both documents.

I am aware that non-compliance or irresponsible behaviour, as per the intent of the BYOx Charter and the Student Code of Conduct, will result in consequences relative to the behaviour.

Student Name: _____

Student Signature: _____ Date: / /

Parent Name: _____

Parent Signature: _____ Date: / /