Woodcrest
State College
Prep to Pathways

Laptop Hire Program

Digitally-enhanced learning for future-ready citizens.

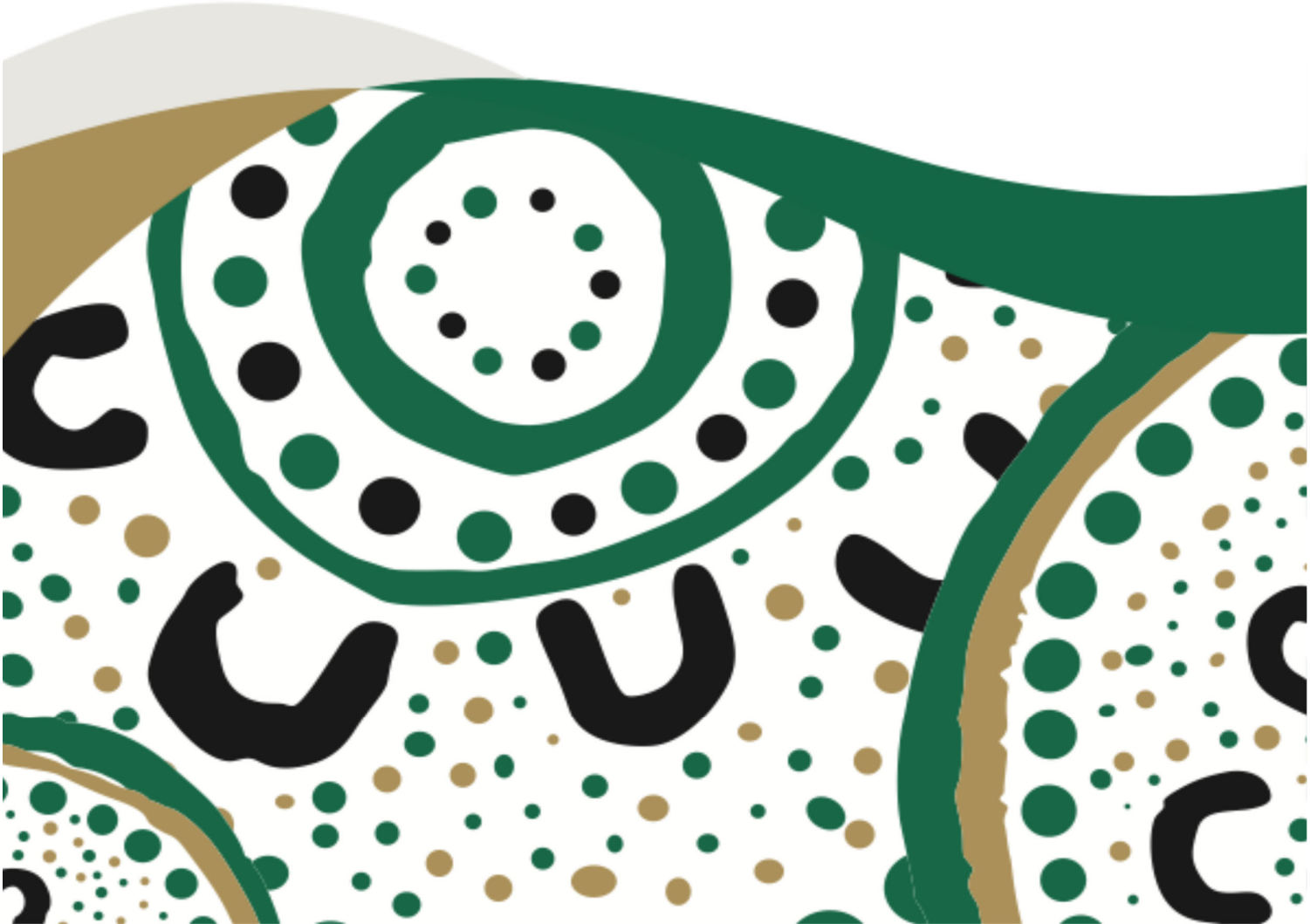


Table of Contents

In addition to our BYOD program, Woodcrest State College offers a hire program for families who may be unable to provide their own device. This initiative ensures that all students have access to essential learning technology, through an affordable option for families.

This allows students who do not have access to their own device to have a true 1-1 experience, enabling them to take work with them, make electronic notes and carry digital textbooks provided by the College.

We have chosen to support a laptop hire program model because it

- Recognises the demand for seamless movement between school and home
- Assists students to improve their learning outcomes in a contemporary educational setting
- Assists students to become responsible digital citizens, enhances the teaching learning process, and supports the achievement of student outcomes

Device ownership

Under the scheme, all laptops are purchased by the college and therefore remain the property of the college. By the college retaining ownership, we are legally allowed to install school software, including the operating system, as well as to manage any warranty and ADP claims. This arrangement is formalised with all parties (parents/carers, students and college) agreeing to the Hire Charter.

At the end of the loan period (12 months), or when the student completes their schooling or transfers from the school, all devices must be returned to the college. If the device is not returned, reimbursement will be sought, or a police report will be lodged for device to be reclaimed.

It is also a requirement of using the device that students provide authorised school staff with access to the device and personal holdings associated with the use of the device if requested.

The Laptop Hire Package

The laptop hire package consists of a 12- 14 inch laptop computer loaded with the schools managed operating environment (MOEv6 windows 11 education edition) protective hard carry case, charger and the departments standard suite of software, including Microsoft Office.

Each laptop will be

- Protected by anti- virus tools and automatic updates
- Able to be connected to the school wireless network for filtered internet and emails
- Able to be used at home and at school for student learning
- Installed with the departments standard suite of software including Microsoft office 365
- Protected by web filtering at school and at home

Device Care

The student is responsible for taking care of and securing the device and accessories in accordance with school policy and guidelines. The school will take no responsibility for any theft or damage. Where the laptop is damaged or stolen, the school may invoice a student's parent/carer for the full cost of repair and replacement.

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 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

Protecting the Screen

- Avoid poking at the screen
- 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

Data Security and Back Up

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 also have the option of saving files to their school One Drive account, allowing for cloud-based storage and access to files both on and off campus.

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, external the service agents may not guarantee the security or retention of the data. For example, the contents of the device may be deleted and the storage media reformatted.

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 online behaviours are easily searchable and may create a permanent record. Interactions within digital communities and environments should mirror appropriate 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 College Student Code of Conduct also supports students by providing school related expectations, guidelines and consequences.

Passwords

Use of the school's ICT network is secured with a username and password. Passwords must meet departmental requirements in order to connect to the network. Passwords 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 hire device which can be shared with parents/carers should they require access to the device at home.

Acceptable 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.

This policy also forms part of the BYOD Charter. The acceptable-use conditions apply to the use of the device and internet both on and off the school grounds.

Communication through the internet and online communication services must also comply with the Woodcrest State College 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 media
- 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.

Misuse and Breaches of Personal Use

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 people 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.

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 carer as soon as 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

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.

Web Filtering

The internet is 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 Internet Use Agreement. To help protect students (and staff) 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 DoE network must also be reported to the school.

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

Parents, carers 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. Students are encouraged to lock the device when not in use.

Intellectual Property and Copyright

Students should never plagiarise information and must 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

The software loaded on the device is licensed to the Department of Education (DOE) or Woodcrest State College. The parent/carer must ensure that the software is not copied, deleted or transferred, without prior written consent from the school. Unauthorised use may breach copyright laws and the parent or caregiver may be held liable for any damages incurred.

Theft & Loss During Hire Term

In the case of loss or suspected theft of an assigned laptop or associated equipment, the school will initiate recovery procedures, however, should a device or the equipment be unrecoverable, the full cost of replacement may be charged to the parent/carer. This includes but is not limited to lost chargers, hard carry cases, USB adaptors and stylus pens.

Warranty & Accidental Damage During Hire Term

All laptops and batteries are covered by a four (4) year manufacturer's warranty which covers manufacturing defects through normal usage and accidental damage. **There is no cover for negligence, abuse or malicious damage. Any software or hardware issues, vandalism, damage, loss or theft of the laptop must be reported immediately to the school.**

The laptop is covered for one Accidental Damage claim per year. Where a laptop is accidentally damaged, the school with initiate and manage a warranty claim with the insurance vendor. For any subsequent accidental damage claims within 12 months, the school will invoice student's parent/carer for the full cost of repair plus labour and postage (if applicable)

Non-warrantable Damage During Hire Term

Non-warrantable damage is where damage to the device is not covered under warranty or accidental damage protection. **Where the school or insurance vendor determines that damage has been intentionally caused to a device or a student has disrespected school property, the full cost of repair or replacement may be charged.**

Some examples include:

- Damage caused by not carrying the laptop in the provided hard carry case
- Any keys being removed from the laptop keyboard due to excessive force applied, and/or additional damage caused by using the keyboard without the keycaps
- Leaving objects (such as headphones or pens) on the keyboard when closing the laptop lid, and as a result the LCD display is damaged (this may be deemed as negligence)
- Leaving objects (such as laptop charger) inside the hard carry case whilst zipped closed, and as a result the LCD display is damaged (this may be deemed as negligence)
- Leaving the laptop unattended and as a result the device is damaged (damage via third party)
- Damaging the device by drawing, scratching, marking the device with a sharp implement, chemicals, makeup etc
- Wilfully twisting/breaking cables in the AC Power Charger lead
- Wilfully damaging the hard carry case in any way (clear ID pocket, zippers, handles, Velcro device fasteners etc)

Responsible Use of Laptop Hire

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

Responsibilities of Stakeholders Involved in Laptop Hire

School

The school will provide:

- Laptop hire 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 minor technical support
- some school-supplied software e.g. Adobe, Microsoft Office 365 printing facilities

Student

The student will:

- participation in Laptop hire program induction
- 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)
- ensure 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)
- seek technical support when required
- maintain a current back-up of data, preferably on OneDrive
- charge the device each night at home in preparation for the following day
- abide by intellectual property and copyright laws (including software/media piracy)
- ensure personal login account will not be shared with another student, and device will not be shared with another student for any reason
- understand and sign the Laptop Agreement

Parents and carers

Parents/carers will:

- acknowledge that the core purpose of the device at school is for educational purposes
- ensure 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)
- seek technical support when required
- understand and sign the Laptop Hire Agreement

The following are examples of responsible use of devices:

- 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/collaborating with students/teachers/parents/carers/experts as part of 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
- being courteous, considerate and respectful of others when using a device
- use the device for private use before or after school
- seek teacher's approval where they wish to use a device under special circumstances

The following are examples of irresponsible use of devices:

- 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
- using a VPN to bypass internet filtering while connected to the school network
- downloading/using software for, distributing or publishing of offensive messages/pictures
- using obscene, inflammatory, racist, discriminatory or derogatory language
- using language/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 services
- sending chain letters or spam email (junk mail)
- accessing private networks (e.g hot spotting phone data) during school time
- knowingly downloading viruses or any other programs capable of breaching the DoE network security
- using the 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 device (including those with Bluetooth functionality) to cheat during exams or assessments
- take into or use devices in exams or during class assessment unless expressly permitted by school staff

Fees

To participate in the school's student laptop hire program, there is a cost involved in the provision and delivery of the device.

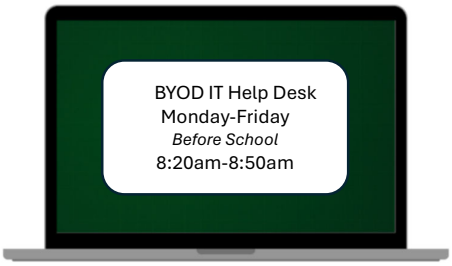
Yearly fee = $200. $50 must be paid in full prior to picking up the laptop. Total fee must be paid in full prior to the end of Term 2.

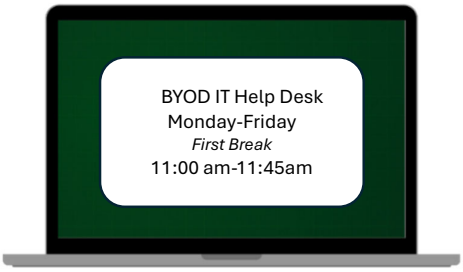
A limited number of student devices are available under our laptop assistance program for families experiencing severe financial hardship. These devices are available for free after consultation with a member of the Corporate Services Team. All devices must be returned 2 weeks prior to the end of the college year.

IT Help Desk

Technical Support Officers are available at the IT Help Desk window in Campus Student Services to assist students by answering technical questions and supporting minor technical issues.

The IT Help Desk is open for students at the following times:





byod@woodcrestsc.eq.edu.au

Laptop Hire Process

1. Complete the students Laptop Hire Agreement/Application Form and External Request for Equipment – Student (EQ-11) Form .
2. Return the agreement forms with payment to the campus administration (please allow a few days for process) or email accounts@woodcrestsc.eq.edu.au.
3. The IT Department will then build the students personal laptop and advise them on daily notices when it is ready for collection. Please note, there will be approximately 1 week wait, between the form being submitted (with payment) and the student receiving the laptop) .
4. Students will need to check daily notices to find out when their device is ready for collection.
5. Visit the IT Help Desk (Campus Student Services Building) to collect your device.
6. Set up device for educational use at school and at home.
7. Bring device to school daily for use in class.