Woodcrest
State College
Prep to Pathways

BYOD @ WSC

Bring Your Own Device at Woodcrest State College

Digitally-enhanced learning for future-ready citizens.

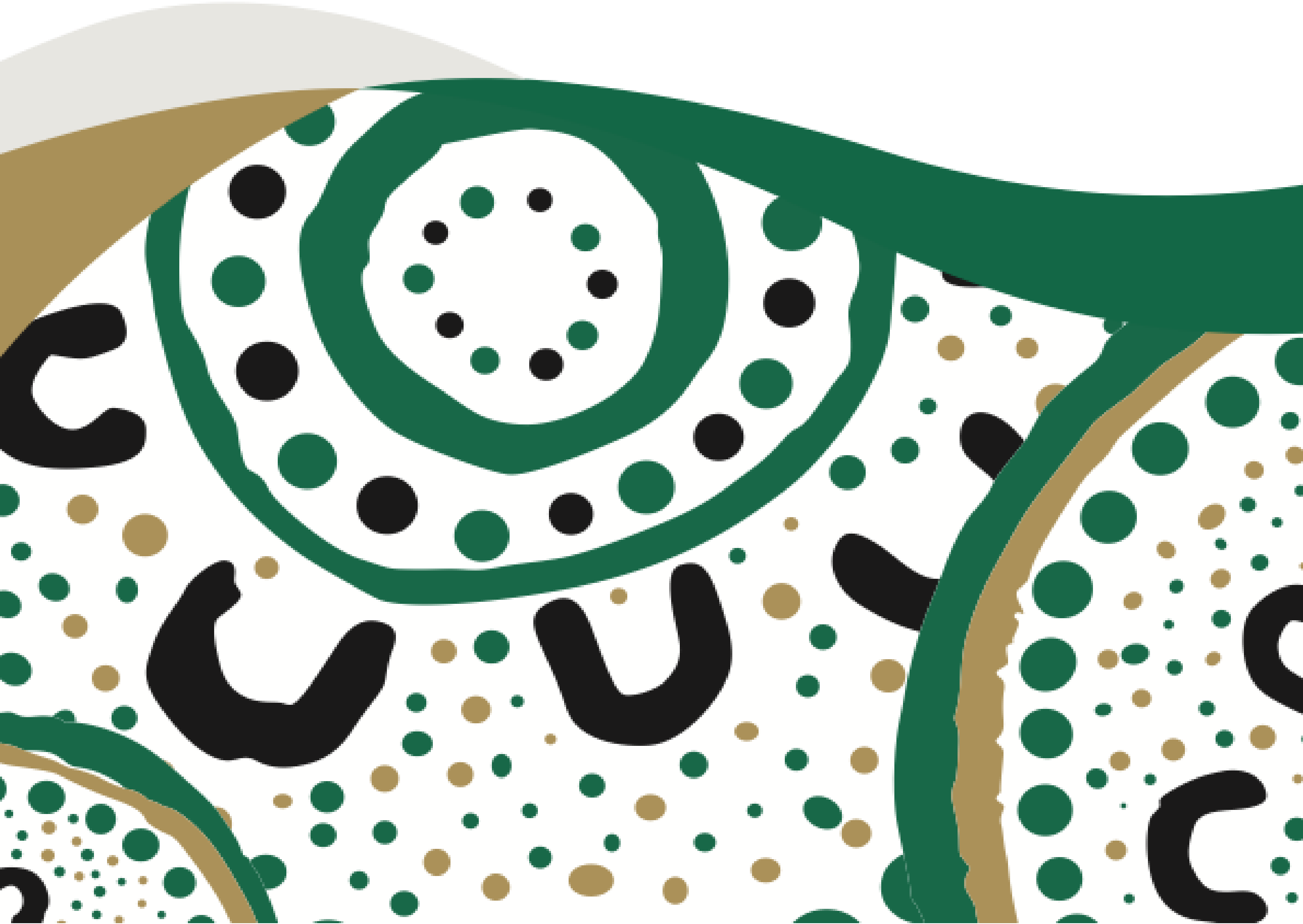


Table of Contents

Bring Your Own Device (BYOD)

Bring Your Own Device (BYOD) at Woodcrest State College is a 1-1 laptop program for students in Years 6-12. It is a term used to describe a digital device ownership model where students use their personally owned device to access the Department of Education's (DoE) Information and Communication Network.

BYOD:

- 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

Access to the DoE ICT network is provided only if the device meets the DoE security requirements which, at a minimum, requires that anti-virus software has been installed, is running and is kept updated on the device. Students are responsible for the security, integrity, insurance and maintenance of their personal devices and their private network accounts.

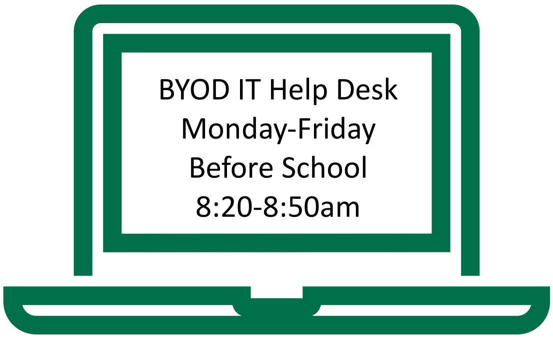
Loan Devices

The College has a limited number of loan devices available for both short and long term for families having trouble meeting the financial costs of the BYOD program. To discuss this option further, please contact the Business Manager via accounts@woodcrestsc.eq.edu.au.

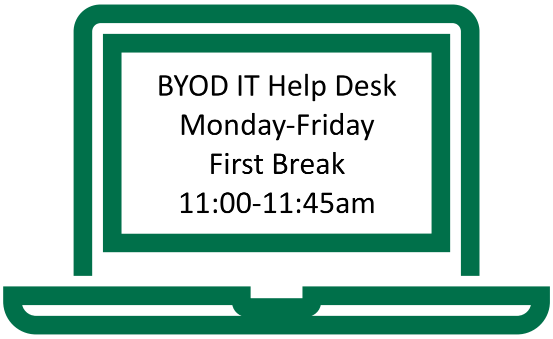
IT Help Desk

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

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



BYOD IT Help Desk
Monday-Friday
Before School
8:20-8:50am



BYOD IT Help Desk
Monday-Friday
First Break
11:00-11:45am

Device Selection and Specifications

Before acquiring a device to use at school the parent/carer and student should be aware of the College's specification of appropriate device type, operating system requirements and software. These specifications have been selected to ensure the device purchased is viable to support your child's learning journey and meets the specifications required to be compatible with DoE operating system requirements and software.

SPECIFICATIONS TO MEET DoE REQUIREMENTS	
Device type	PC Laptop, 2 in 1 Tablet PC or Mac Laptop
Processor	Intel i3/Dual Core Pentium or higher (ARM **not currently supported**)
Graphics Card	Intel HD Graphics 5000 (or equivalent)
RAM	4GB RAM minimum
Battery Life	6 hours+ on balanced power mode
Hard Drive	128GB or above (note: we recommend a 256GB Solid State Drive for increased durability and speed)
Screen Size	11" Screen or above
Operating System	Windows 11 Mac OSX 11.7 (Big Sur) or higher **Windows 10 (and Prior), Windows 11 in S-Mode Android, Chromebooks, Surface RT and other devices that run Linux are NOT SUPPORTED on the DoE network**
Wireless	Capable of 5GHz
Software	Internet Browser e.g. Microsoft Edge, Google Chrome, Firefox, Safari
Features	Keyboard, USB Port 3.0, headphone port
Virus Protection	Windows Defender or other Virus Protection (Trend Micro is NOT recommended)
Accessories	Wired headphones & Protective Case

SPECIFICATIONS REQUIRED FOR TECHNICAL SUBJECTS: (MEDIA, MEDIA ARTS IN PRACTICE, VISUAL ARTS, VISUAL ARTS IN PRACTICE, FILM TELEVISION & NEW MEDIA, INDUSTRIAL GRAPHICS SKILLS, DESIGN)	
Processor	Intel core i5/i7-2.3GHz or equivalent (ARM **not currently supported**)
Graphics Card	2GB Dedicated Graphics
RAM	8GB or greater
Battery Life	8hrs or greater
Hard Disk	256GB or higher SSD
Screen Size	14" minimum
Operating System	Windows 11 (note: Windows S Mode is not compatible)
Software	As per subject requirements outlined in subject selection handbook
Warranty	Extended to 3 or 4 years with accidental damage protection
Features	Keyboard, USB Port 3.0, headphone port, protective carry case
Virus Protection	Windows Defender or other Virus Protection (Trend Micro is NOT recommended)
Accessories	Wired headphones & Protective Case

Windows 10 (and Prior) are not supported on the BYOD network. Surface RT, Windows 11 in S-Mode, Linux, Chromebooks and Android are NOT COMPATIBLE with the BYOD network. Devices that have less than 128GB storage are also not supported as they do not have enough available free space to install required software. Additionally, no SMART PHONES are allowed on the BYOD network.

Windows 11 S-Mode is a version of Windows 11 designed for security and performance, exclusively running apps from the Microsoft Store. For the device to connect to the BYOD Network, the device will need to be switched out of S-Mode. Instructions are available on the Microsoft support website at: https://support.microsoft.com/en-us/help/4456067/windows-10-switch-out-of-s-mode.

Device Care

The student is responsible for taking care of and securing the device and accessories in accordance with college 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 the device's inclusion in a home and contents insurance policy. It is advised that accidental damage and warranty policies are discussed at the point of purchase to minimise financial impact and disruption to learning should a device not be operational.

General Precautions

- Take precautions for device when near food or drink
- 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 night at home in preparation for the following day
- Turn the device off before placing it in its bag

Protecting the Screen

- Avoid poking at the screen — even a touch screen only requires a light touch
- 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

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 DoE ICT network. Students also have the option of saving files to their school OneDrive 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, should any repairs need to be carried out, external 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 BYOD 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

Schools may recommend software applications to support curriculum needs of particular subjects. Parents/carers 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 graduation, transfer or cancellation of enrolment.

Microsoft 365

Microsoft 365 allows students to install the Microsoft suite of software at no cost to families. Microsoft 365 can be installed at home by following the Microsoft Installation guide.
https://woodcrestsc.eq.edu.au/Supportandresources/Formsanddocuments/Documents/BYOD/installation-step-by-step-guide.pdf

Adobe Creative Cloud

This software is available, free of charge, to students studying in specific subjects at the school. At the beginning of each year, the school will assign a named-user Adobe licence to eligible students. The licence is valid until the end of the year and continues for the duration of the student's enrolment at Woodcrest State College while studying the subjects mentioned above. Students will need to download their required Adobe applications at home using the instructions they receive from school. Adobe applications cannot be downloaded and installed at school due to the large size of the package and the lengthy installation process.

Microsoft Family

If you are concerned about the amount of screen time your child is accessing, we strongly recommend setting Microsoft Family for Windows laptops. **The onboarding process must be completed prior to setting Microsoft Family -** https://www.microsoft.com/en-au/microsoft-365/family-safety.

Responsible Use of BYOD

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 BYOD

School

The school will provide:

- a BYOD 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 365
- printing facilities

Student

The student will:

- participate in BYOD program induction
- acknowledge that the core purpose of device at school is for educational purposes
- care for device
- demonstrate 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 BYOD 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
- install required software including anti-virus software
- provide a protective sleeve or case for the device
- obtain an adequate warranty and insurance for the device
- understand and sign the BYOD Charter 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 (eg 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

In addition to this:

- information sent from our school network contributes to the community perception of the school, therefore, all students using our ICT facilities are expected 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 have permission before copying files from another user, as 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 carers 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 college 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 and students have a responsibility to incorporate these safe practices in their daily behaviour at school

The school's BYOD program supports personally owned devices in regard to:

Printing

Internet

File access and storage

School network

The school's BYOD program DOES NOT support personally owned devices in regard to:

Technical support

Charging of devices at school

Security, integrity, insurance & maintenance

Private network accounts