BYOD @ St Martins

Bring Your Own Device option - Years 10 -12

What is Bring Your Own Device (BYOD)?

Bring Your Own Device (BYOD) refers to where students bring a personally owned device to school for the purpose of learning. At St Martins Lutheran College this is our preferred method for students to access electronic resources in Years 10 to 12.

With classroom teacher approval, students may use their own devices to access the internet and collaborate with other students. BYOD allows students to use the technologies that are most appropriate for their personal learning programme. Note: this may mean that a student continues to use the Chromebook they were issued with in Year 7.

Additional information can be found in:

- BYOD Portal
- Chromebook Handbook (given to Years 7-9)
- Information and Communication Technology Policy
- Student ICT User Agreement
- (FAQs) – at the end of this document

If you require any further support, please contact the College.

The BYOD Portal is a means of ordering a laptop that will be suitable for most SACE subjects at Stage 1 and 2. Some subjects may have specific requirements depending on the nature of the subject. If unsure, please speak with the relevant subject teacher.

The portal is offered as a service by the school in conjunction with a provider and may offer advantages in terms of simpler purchasing, competitive pricing and stream-lined servicing of machines. Additional warranty protection may also be purchased through the portal. It must be remembered that unlike the Chromebook devices issued by the school, any devices purchased through the portal are the property and responsibility of the family purchasing them. Where families are looking for a different option outside of what is offered by their child's existing Chromebook or portal options, then the devices on the portal serve as a minimum specification in terms of processing power and battery life.

The Information and Communication Technology Policy describes the responsibilities of all users of the school ICT infrastructure and internet connection.

The Student ICT User Agreement is an annual agreement made by users making use of school ICT infrastructure.

BYOD @ St Martins

- All students have access to the St Martins Lutheran College wireless network including access to the internet as per the conditions set out in the Student ICT User Agreement.
- Only devices approved for connection by the St Martins Lutheran College ICT Department may be used.
- All BYOD devices must only be connected to the school's wireless network. Direct connections using other means such as LAN or hotspots are prohibited unless a specific exemption is approved by the ICT Department.
- Devices should be brought to school fully charged. Chargers are discouraged from being used at school. Only electrically tagged equipment can be used at school in areas where they do not present a hazard.
- No student shall establish a wireless ad-hoc or peer-to-peer network using their electronic device or any other wireless device while on school grounds.
- Voice, video, and image capture applications may only be used with teacher permission and where relevant to the learning environment, whilst being respectful of the rights and permission of others.
- The owner of the electronic device is the only person allowed to use the device and their unique username and password associated with the device. In the event that a student believes that their password has been compromised, they should immediately see the St Martins Lutheran College ICT Department to have their password changed.

These guidelines apply to any device used for personal learning brought into school, except for mobile phones. Students bringing a mobile phone to school do so in compliance with the College Mobile Phone Policy and procedures.

Purpose

This document outlines the standards, procedures, and expectations for all users connecting personally owned devices to the St Martins Lutheran College network. It also applies to any software or hardware not owned or provided by the school.

The College currently recommends laptops and Chromebooks as the preferred devices, due to their compatibility with the school network and the hardware and software requirements of learning programs. Other devices may have limited or no access to the College's network

and services. Only devices approved for use are permitted to connect to the school's wireless network.

While recognising the value of ICT tools and services, it is essential to safeguard the integrity, confidentiality, and security of all school data. All staff and students are expected to adhere to College policies to minimise the risks associated with potential security threats.

Threat	Potential Risks
Device loss	Devices need to be password protected to minimise the loss or theft of work files. Students need to ensure that their devices are securely stored when not in their possession.
Data loss/theft	Users need to ensure that sensitive data is not uploaded onto devices.
Malware	Viruses, Malware, Trojans, worms, spyware and other threats are a risk to our network where personal devices are not adequately protected from malware.
Compliance	Loss or theft of personal or confidential data could expose the school to risk of non-compliance with various child protection, identity theft and privacy laws, so employees and students need to always maintain compliance with this and related policies.
Software Vulnerabilities	The device's operating system, and any installed software, should always be updated to the latest available version to help minimise the risk of software vulnerabilities being exploited.

Monitoring of Devices Connected to the School Network

The Principal of St Martins Lutheran College retains the right to make final determinations about what constitutes appropriate content and has overarching responsibility for the appropriate access to and use of the school's ICT infrastructure, network, and data management. This includes the authority to monitor, access and review all use of school resources and infrastructure, including personal web browsing and emails sent or received using the school's ICT facilities.

As part of the College's quality assurance, data integrity and security processes, audit trails will be established to track the attachment of external devices to the school network where a suspected breach or misuse of ICT resources has occurred. This monitoring may include dates, times, and duration of access to verify that school data and security have not been compromised.

Consequences for breaches will be determined by the Principal or delegate and may include restricting an individual from bringing a personal device to school. The Principal or delegate also reserves the right to audit, at any time, any material on equipment owned or leased by the College, as well as to audit privately owned ICT devices or storage media used at school or during any school-related activity.

Connectivity of all student-owned devices will be centrally managed by the St Martins Lutheran College ICT Department. Device configurations will follow the guidelines established to protect and secure school data, information systems and storage. Configuration requirements may include password protection, encryption, and other controls necessary to isolate and safeguard sensitive information accessed from, or stored on, personal devices or the school network. Students are expected to uphold the same security protocols when connecting to non-school equipment to help prevent loss, theft or unauthorised access to information on their devices.

ICT for Personal Learning and Acceptable Use

It is the responsibility of every student and employee of St Martins Lutheran College to ensure that our ICT resources are never used to abuse, vilify, defame, harass, degrade or discriminate against others as per the ICT User Agreement.

The following access controls must be observed at all times:

- All users must employ reasonable security measures including, but not limited to, passwords, encryption, physical controls and safe storage of personal devices whenever they contain school data.
- Students may not use an audio recording device, video camera, or camera (or any device with one of these, e.g. mobile phone, laptop, tablet, etc.) to record media or take photos during school unless they have teacher permission and the permission of whom they are recording.

All students should use their lockers to store phones or other valuables.

In special cases such as Physical Education lessons where the potential exists for students to ask staff to look after valuables, if the staff member elects to take the valuables no responsibility for their security will be accepted. The responsibility for student valuables remains with the student and secure lockers are provided for this purpose. All students are responsible for keeping their lockers secure.

Selecting Devices

Which should I bring?
In conjunction with Learning With Technology, we have a Parent Online Purchasing Portal where devices can be purchased. It should be noted that devices do not need to come from this portal. Also, a reminder that Chromebooks received in Year 7 or when enrolling can continue to be used.

The Purchasing Portal is located via the link on the St Martins Lutheran College Website, in the Parents Portal. A range of laptops and Chromebooks are available at education discounted prices.

When purchasing these devices, you have the option to take out accidental damage protection (highly recommended unless the device can be covered by your existing household contents insurance), other options will also be available to purchase at the same time (carry bag, mouse, external hard drive etc.).

The St Martins Lutheran College ICT Department can assist with warranty repair arrangements for devices purchased through the portal should it be required.

It is expected that if devices are not purchased through the portal, they will meet or exceed the technical specifications of the devices on the portal.

Anti-Virus Software

A current and up to date anti-virus application MUST be installed and active on all devices connected to the St Martins Lutheran College network. Any device found not to have current antivirus software will be blocked from the network.

There are many effective free or low-cost Anti-Virus products available – please see the St Martins Lutheran College ICT Department if you require further information.

Technical Support

Network Connection

Students need to connect to the school's wireless network by following the instructions provided by the St Martins Lutheran College ICT Department. Only approved devices can be connected.

Students who are having technical issues connecting their device can visit the St Martins Lutheran College ICT Department Office (normal support is from 8:45am to 3:30pm during school terms – outside of these times by arrangement)

An initial scheduled time will be made in Home Group to help support students to connect their device during the first week of each term.

Charging

It is the responsibility of the student to bring their device to school fully charged. Devices can only be charged at school using electrically tagged chargers in locations that do not create hazards.

Printing

Printing will be supported for all devices via PaperCut. All prints are logged and charged to the student when printed.

Insurance and Liability

St Martins Lutheran College does not accept liability for any loss, damage or theft of any device that is brought to school under the program. The responsibility for the storage, safe-keeping and care of the device is the responsibility of the device owner. The school's insurance policy does not apply to these devices; instead these are covered by the user's

insurance policy. As such it is strongly recommended that families ensure that the details, such as serial numbers and receipts of purchase for these devices are stored securely at home for insurance purposes.

Data Loss and Backup
Students should ensure that their files are backed up. Cloud-based storage is recommended for most files.

FAQs

What is Bring Your Own Device (BYOD)?
Bring Your Own Device (BYOD) refers to technology models where students bring a personally owned device to school for the purpose of learning.

Is student internet monitored?
Internet access is filtered whilst students are using the school's network.

Where do I go for support?
If students are not able to connect to the school's wireless network, students can visit the St Martins Lutheran College ICT Office between 8:45am-3:30pm (note the office is not always attended) when they don't have lesson commitments.

My laptop was damaged/stolen when I brought it to school. Who should I contact?
Bringing your own device to school can be useful; however, some risks are involved as well. It is always a good idea to record the device's serial number in case of theft and have your own insurance. The school is not responsible for the theft of a device, nor is the school responsible for any damage done to the device while at school.

If a theft occurs, you should speak with your Home Group teacher to make them aware of the issue. Parent/Caregivers will need to ensure that their devices are covered for other situations under their own insurance policies.

Can my child use the printer from this device?
Devices purchased through the Portal will be able to print. Most other devices will be able to print through the St Martins Lutheran College network.

What happens to students' work if the computer hard drive fails or the computer is stolen?
We recommend and encourage students to use additional backup measures to keep their documents safe, such as external hard drives, USB drives or cloud storage.