ST MARY'S COLLEGE

2025 HANDBOOK

BRING YOUR OWN DEVICE (BYOD) PROGRAM

www.stmaryscollege.vic.edu.au

November 2024

Contents

NOTE:
This document should be read in conjunction with:

a) the College *'Information and Communication Technology (ICT) Policy'*;
b) the College '*Annual Student ICT User Agreement'; and*
c) the College 'Bullying Prevention and Intervention Policy';
d) Cyber Safety Policy
e) Harassment (Student Against Student) Policy and
f) the College 'Student Behaviour Management Policy'.

HOW TO
CONTACT US

Telephone

+ 61 3 9529 6611

Email

enquiries@stmaryscollege.vic.edu.au

fees@stmaryscollege.vic.edu.au

Website

www.stmaryscollege.vic.edu.au

BYOD Online Shop

https://shop.compnow.com.au/school/stmarys-college

Parent Portal

Parent Access Module PAM (SIMON) – login HERE

Postal address

PO Box 258
ST KILDA VIC 3182
AUSTRALIA

WHAT IS THE **BYOD PROGRAM?**

The Bring Your Own Device (BYOD) Program at St Mary's College is designed to support innovative learning for students through the use of personal devices and technology.

St Mary's College requires students to provide their own electronic device for student learning purposes. The BYOD program provides an opportunity for families to obtain electronic devices at educational pricing.

Students are required to have one of the devices listed in this booklet. It is not a requirement to purchase through the BYOD portal, however, the pricing is generally discounted compared to other retail outlets.

It will be the Parents' responsibility to make sure the device is insured under their Home and Contents insurance.

The advantage of purchasing the device from the BYOD Portal is that the devices not only have 3 years' warranty, but also have the option of purchasing Accidental Damage Protection ("ADP") insurance. The ADP insurance protects the device against repair costs for loss and physical damages that are not generally covered by standard warranty terms and conditions.

BYOD PROGRAM **DEVICES**

The College has negotiated special education pricing on the specified devices in order to provide families with the best available price. The St Mary's College BYOD Program provides the opportunity to purchase the following devices.

Lenovo 300w G4 11.6" TS N100 8GB 256GB Win11Pro SSD

The Lenovo 300w Yoga Gen 4 convertible PC is powered to support big work from little learners, thanks to its Intel® processors and plentiful memory and storage.

Features:

- 11.6 HD MultiTouch 250 nits Touchscreen display
- Intel N100 Processor (4 Cores, Up to 3.4Ghz)
- 8GB LDDR5-4800 Onboard Memory
- 256GB SSD
- Integrated Graphics
- Intel AX201 2X2AX Wifi + Bluteooth
- 65W USB-C 3 Pin
- 3 Cell 47WH
- 720P HD Camera
- Lenovo Digital Pen / stylus
- Windows 11 Pro

Ports:

- 1x USB-C 3.2 Gen 1
- 1x HDMI 1.4
- 2x USB-A 3.2 Gen 1
- 1x Audio Jack

Price: $781.53 inc

HP Probook 445 G11 14" TS Ryzen 5 7535U 8GB 256GB SSD Win11P

The HP ProBook 445 G11 Laptop with an integrated infrared (IR) touchscreen display and an AMD Ryzen 5 7535U processor is the ideal choice for business professionals seeking a blend of affordability, performance, and intuitive control.

Features:

- 14" WUXGA (1920 x 1200), Touch
- AMD Ryzen 5 7535U Processor
- 8GB DDR5 RAM
- 256GB SSD
- AMD Radeon 660M Graphics
- 65 W USB Type-C Adapter
- Windows 11 Pro
- 1-Year Onsite Warranty

Ports:

- 2 USB Type-C 10Gbps signaling rate (USB Power Delivery, DisplayPort 1.4)
- 1 USB Type-A 5Gbps signaling rate (USB Power Delivery)
- 1 USB Type-A 5Gbps signaling rate (charging)
- 1 HDMI 2.1
- 1 Stereo headphone/microphone combo jack
- 1 RJ-45

Price: $1,360.19 inc

HP Probook 465 G11 16" TS Ryzen 5 7535U 16GB 512GB SSD Win11P

Unleash peak performance, intuitive control, and ample storage with the HP ProBook 465 G11 featuring a stunning 16-inch WUXGA touchscreen display.

Features:

- 16" WUXGA (1920 x 1200), Touch
- AMD Ryzen 5 7535U Processor
- 16GB DDR5 RAM (2 x 8GB)
- 512GB SSD
- 65 W USB Type-C Adapter
- Windows 11 Pro
- 1-Year Onsite Warranty

Ports:

- 2 USB Type-C 10Gbps signaling rate (USB Power Delivery, DisplayPort 1.4)
- 1 USB Type-A 5Gbps signaling rate (USB Power Delivery)
- 1 USB Type-A 5Gbps signaling rate (charging)
- 1 HDMI 2.1
- 1 Stereo headphone/microphone combo jack
- 1 RJ-45

Price: $1,488.40 inc

Apple MacBook Air 13.6" M2 8C CPU/GPU 16GB 256GB SSD Space Grey

MacBook Air sails through work and play. You can express yourself and get things done effortlessly with Apple Intelligence. And with up to 18 hours of battery life, you can take the ultraportable MacBook Air anywhere and power through whatever you're into.

Features:

- 13.6-inch (diagonal) LED-backlit display with IPS technology
- 2560-by-1664 native resolution at 224 pixels per inch
- 500 nits brightness
- Apple M2 chip
- 8-core CPU with four performance cores and four efficiency cores
- 8-core GPU
- 16GB unified memory
- 256GB SSD
- Backlit Magic Keyboard
- Wi-Fi 6 (802.11ax)
- Bluetooth® 5.3
- 30W USB-C Power Adapter

Ports:

- MagSafe 3 charging port
- 3.5-mm headphone jack
- Two Thunderbolt/USB 4 ports with support for:
- Charging
- DisplayPort
- Thunderbolt 3 (up to 40 Gbps)
- USB 4 (up to 40 Gbps)

Price: $1,460.40 inc

COST OF **PARTICIPATION**

There is no additional cost to Parents beyond the purchase of the device. A portion of the College Tuition Fees and Levies will partially offset some of the following costs:

- Access to the College wireless network
- Access to our fast internet connection
- Access to Microsoft Office 365 on up to 5 devices (includes student email)
- Access to Adobe Creative Cloud (Design and Web Premium)
- Technical support for warranty and out of warranty logging and follow-up (for devices purchased through the College BYOD Portal)
- 24/7 student and parent access to our Learning Management Systems (SIMON)
- Access to on-line textbooks and learning apps

ASSISTANCE **TO OBTAIN A DEVICE**

Families experiencing financial difficulties, are encouraged to contact the College Business Manager to discuss options.

PRIVATE **DEVICES**

The primary educational device in use at the College is noted in the 'BYOD Program Devices' section above. Other multimedia devices such as smartphones may only be permitted as a supplement to the student's primary educational device, and only with the approval of the College and in accordance with the St Mary's College Information and Communication Technology (ICT) Policy.

Other devices such as wireless routers, USB modems and Wi-Fi modems or tethering from smartphones is strictly prohibited.

Any use of a device other than the primary educational device will only be approved in exceptional educational situations or as agreed by the College.

PROCESS AND GUIDELINES **FOR PARTICIPATION**

Prior to the commencement of the school year:

- Parents will receive this BYOD Program Handbook outlining the details of how the BYOD Program operates.
- Students are required to sign the *'Annual Student ICT User Agreement''.* By signing this document, students agree to adhere to the College 'Information and Communication Technology (ICT) Policy'. This policy is available to students and parents via the SIMON/PAM student and parent portals.
- No student may use the College ICT network, equipment or devices unless the *'Annual Student ICT User Agreement'* is signed.
- Students will be instructed in the use of the devices, the College Learning Management System – SIMON, and any other software, when they commence school.

The device must be brought to school fully charged and ready for use in classes each day. There will be limited opportunity for charging student devices at school.

Student devices must be taken home each evening and must not be left in the student's locker or classroom overnight.

LOSS AND DAMAGE **POLICY**

Students and their parents/guardians, are responsible for any loss or damage to BYOD/personal devices. The College will not take responsibility for damage to, or loss of, student property.

Parents must ensure that their child's device is covered under their home and contents insurance policy at all times.

It is the user's responsibility to report lost or stolen devices to the nearest police station and provide the insurer with a crime report number and claim for a replacement on their home, contents or car insurance.

If the device is taken overseas, please ensure that it is covered by travel insurance.

If a device is damaged in any way during class time, students should report this immediately to their classroom teacher. For all other damage sustained on school grounds, notification should be made to the student's Pastoral Care teacher.

CYBER **PROTECTION**

Please see the College Information and Communication Technology (ICT) Policy for details of College cyber safety protocols and procedures. Students are required to comply with the College Cyber Safety Policy.

ONSITE TECHNICAL **SUPPORT**

St Mary's College offers ICT support services to devices purchased through the College BYOD Portal.

Devices purchased via the College BYOD Portal will be diagnosed and sent by us to our repair agent, if required. Parents/guardians are also able to book their child's device repair directly with the Compnow retail centre in Clayton or Apple service centre directly if they so choose.

Devices purchased outside of the College BYOD Portal will be diagnosed by the College ICT support services, however, parents/guardians will be responsible to return the device to the place of purchase for any further repairs or queries.

SOFTWARE, COPYRIGHT **AND INTELLECTUAL PROPERTY**

St Mary's College licensed software is subject to copyright and must not be distributed or copied in any way. When a student is no longer enrolled at the College, it is their responsibility to remove any St Mary's College installed software.

Students may install their own software as required. This software must be legally purchased with a user license. The software must not be malicious, offensive, or breach copyright laws. Students should avoid installing registry cleaners and PC optimizer programs, as they have the potential to damage the operating system. St Mary's College internet filtering does prevent some private software such as P2P, VPN applications and online games from being used.

NON-SCHOOL **APPLICATIONS**

Non-school applications include apps such as games, music, movies, photographic content, etc. The College does not object to the installation of non-school content on devices, provided that the installed content:

- is appropriately licensed (i.e., does not breach copyright and intellectual property laws – this includes video and music downloads);
- is ethically and morally acceptable including consideration of College codes of conduct and behavioural standards, age appropriate ratings and any privacy issues;
- does not affect the efficient functioning of the devices for educational purposes (i.e., they do not interfere with the speed and storage capacity of the device or problems that might arise from increased battery use).
- does not affect the College wireless network;
- does not interfere with classroom learning programs or contradict College behavioural expectations (i.e., they may not be used during school hours except with the express permission of a staff member).

In particular, while some games have educational benefits and will be used under teacher direction, other games have little educational merit. As a result:

- The use of network games is prohibited.
- Ad-hoc networks are not to be formed.

INTERNET **USAGE**

Students can access the Internet through the College's wireless network while on site. Access to the internet through the College network will be monitored and is subject to categorised filtering.

Access to the College's wireless network is only permitted in accordance with the College Information Communication Technology (ICT) Policy.

USERS **AND SECURITY**

Each student will be issued a network username and password to access the College's wireless network, Office 365 and the Adobe Creative Cloud suite, SIMON Management System as well as other relevant applications. This password cannot be divulged to any other party under any circumstance. Sanctions will be taken against any sharing of passwords and students will be responsible for sites accessed using their account irrespective of whether they personally accessed the site or not.

Our network audit logs contain information on the user logging in, the computer which is attempting to log in and various other parameters. This information can, and will, be used to track user access and usage. Outside access will be monitored and referred to the Police.

SOCIAL **NETWORKING**

The use of some Social Networking applications has educational benefits. These sites allow users to interact with other users, including web-based communities, hosted services, web applications, social-networking sites (Facebook, Twitter etc.), video-sharing sites, wikis and blogs.

However, many Social Networking applications can be unproductive and distracting to student learning.

The use of Social Networking applications is only permitted in accordance with the College Information and Communication Technology (ICT) Policy. It is our policy that members of the College community, including students will:

- only use social media applications at school with the express permission of a staff member;
- use social media in a respectful and responsible manner;
- refrain from acting in such a way that brings the College into disrepute or in a way that harms members of the College community;
- not insult or present offensive or inappropriate content; and
- not misrepresent the College or any member of the College community.

When using social media, students are expected to ensure that they:

- Do not use social media applications at school without the express permission of a staff member;
- Respect the rights and confidentiality of others;
- Do not impersonate or falsely represent another person;
- Do not use avatars or other means of hiding or misrepresenting their identity;
- Do not bully, intimidate, abuse, harass or threaten others;
- Do not make defamatory comments;
- Do not use offensive or threatening language or resort to personal abuse towards each other or members of the College community;
- Do not post content that is hateful, threatening, pornographic or incites violence against others;
- Do not harm the reputation and good standing of the College or those within its community; and
- Do not film, photograph or record members of the College community without express permission of the College or use film, photographs or recordings without express permission of the other parties.

A failure to abide by the above expectations may constitute bullying.

NETWORKS AND **NETWORK SECURITY**

Access to the College's wireless network is only permitted in accordance with the College Information Communication Technology (ICT) Policy.

Ad-Hoc Networks

Ad-hoc networks (the creation of a standalone wireless network between two or more devices) are strictly forbidden while at school. The St Mary's College network security system will scan for, remove and report on any ad-hoc networks detected.

Wired Networks

Students are forbidden to plug any device into St Mary's College wired network. St Mary's College network security system will scan for and report on any non-school devices plugged into our wired network.

Hacking

Hacking is a criminal offence under the Cybercrime Act (2001). Any hacking attempts will be forwarded to the Police.

Packet Sniffing

Any type of software or hardware device designed to capture or view network data/packets is forbidden. Any student detected capturing network traffic will be suspended. The St Mary's College network security system will scan for and report of any device capturing packets.

APPROPRIATE **USE OF ICT**

The Network Manager maintains computers/devices and the network so that they operate effectively, and that the resources needed are available.

Guidelines in relation to appropriate use of devices are contained in the St Mary's College *'Annual Student ICT User Agreement',* the College Information and Communication Technology (ICT) Policy, the Student Use of Mobile Phones Policy, Cyber Safety Policy and other associated policies.

The following guidelines are in keeping with these policies, and are outlined to ensure all users are able to access the latest research available with the latest technology in an acceptable and safe learning environment:

- Users will avoid sites with content that is violent, racist, sexist, pornographic, dominated by offensive language and/or illegal in any way.
- Engaging in chat lines or downloading files is not permitted unless forming part of legitimate class activity guided by the teacher of that class.
- The Federal Communications Act determines guidelines for appropriate use.
- Inappropriate use of the internet and email is a serious matter and can have significant consequences, e.g., sending a message over the internet using someone else's name.
- Passwords should remain confidential. No user should log-on as another student using their password.

- It is the responsibility of students to maintain sufficient credit in their printing account to allow subject related tasks to be carried out.
- Do not remove files or folders that have been installed to the hard disk or network.
- Do not use inappropriate or offensive names for files or folders.
- Do not bring to school, or use, games or any other materials which may be offensive to others.
- Do not engage in cyber-bullying or e-crime.
- No device (or mobile phone) with camera capabilities are to be used in change rooms or toilets.
- Under privacy legislation, it is an offence to take photographs of individuals without their expressed permission and place these images on the Internet or in the public forum.

CYBER **BULLYING**

Principles

- Every person has a right to be treated with respect and as a worthwhile individual.
- Every member of the College community has a right to a safe environment, free from bullying.
- Bullying behaviour, including cyber-bullying, seriously undermines the ethos of the College, is not acceptable, and will not be tolerated.
- If a student is bullied, they have the right to be heard.
- All bullying matters will be taken seriously and will be investigated with discretion, confidentiality and sympathy.
- Positive action will be taken and where necessary disciplinary action will be put in place.

Definition

Technology provides individuals with a powerful means of communicating instantly with others in both positive and negative ways. Cyber bullying is bullying which uses technology as a means of victimising others. It is the use of an internet service or mobile technologies, such as email, chat room discussion groups, instant messaging, webpages or SMS (text messaging) with the intention of harming another person.

Cyber may include, but is not limited to:

- Online bullying – the ongoing abuse of power to threaten or harm another person through the use of technology.
- Sexting – the sending or posting of provocative or sexual photos, messages or videos online.
- Identity theft – the fraudulent assumption of a person's private information for their personal gain. (Students are exposed to these risks as they may be unaware of the safety issues surrounding their digital footprint).
- Predatory behaviour where a student is targeted online by a stranger who attempts to arrange a face to face meeting, in an attempt to engage in inappropriate behaviour.
- The use of communications that seek to intimidate, control, manipulate, put down or humiliate the recipient.

Cyber bulling activities can include flaming (repeated negative messages), trolling, sexual or racist harassment, denigration, impersonation, trickery, exclusion and cyber stalking. The targeted person often feels powerless and may need help.

Policy

The College's cyber bullying policy is contained in our 'Information Communication and Technology (ICT) Policy' and 'Bullying Prevention and Intervention Policy'.

Bullying behaviour, including cyber-bullying, seriously undermines the ethos of the College, is not acceptable, and will not be tolerated.

Any breach of the College's Information and Communications Technology (ICT) Policy, Bullying Prevention and Intervention Policy or related policies, will be considered by the College and will be dealt with on a case by case basis. All reports of cyber bullying, hacking and other technology misuses will be investigated fully and may result in a notification to Police where the College is obliged to do so. Student breaches of these policies will result in disciplinary action in accordance with the College Student Behaviour Management Policy and procedures. Sanctions for students may include, but are not limited to, the loss of ICT privileges, detention, suspension or expulsion from the College.

Students and parents should be aware that in certain circumstances where a crime has been committed, they may be subject to criminal investigation by Police over which the College will have no control.

ELECTRONIC **CRIME**

Cyber bullying may involve varying levels of severity, ranging from occasional messages to frequently repeated and highly disturbing threats to a person's life.

Cyber bullying can therefore be an e-crime, a fact often not clearly understood by those involved.

E-crime occurs when a computer or other electronic communication devices (e.g., mobile telephones) are used to commit an offence, are targeted in an offence, or act as a storage device in an offence.

Students and parents should be aware that in certain circumstances where a crime has been committed, they may be subject to criminal investigation by Police over which the College will have no control.

BACKUP **AND DATA STORAGE**

It is important to keep backups of critical student work. The main option for student backups is to install and use Microsoft OneDrive which comes as part of the Office 365 suite. OneDrive is free and allows up to 1TB worth of storage on Microsoft Cloud. This means that in the event of losing a device the student is still able to access a copy of their work. St Mary's College will not be held responsible for lost work due to a failure to backup.

STUDENT **PRINTING**

Student work will most often be electronically submitted. If students are requested to hand up a printed version, printing facilities will be available in the College Libraries.

There is a cost to printing. An amount of $20 will be automatically added to the students account at the start of each semester. Printing is charged at a rate of 10c per black and white print and 20c per colour print. If the student requires further credit, Parents/Guardians are required to make a payment online via our online payment portal and this will be added to the printing account.

DEVICE **CARE**

Looking after the device is the student's full responsibility. Here are some tips in helping students achieve this:

- Always keep the device in its protective case when not in use.
- Keep devices locked away in designated lockers during breaks.
- Never leave your devices unattended.
- Never leave any items in between the keyboard and screen (as this is the most common way of screen breakages occurring).

BYOD / ICT **ENQUIRIES**

Should parents or students have any questions in relation to the BYOD Program or require ICT support, please contact the College ICT Manager, Sam Babakhani via email: **itsupport@stmaryscollege.vic.edu.au** or (03) 9529 6611.

Questions in relation to the recommended devices should be directed to Compnow via email: school.portal@compnow.com.au or call 1300 077 973