St Peters
Lutheran College

St Peters BYOT

Program Overview | Years 7-12

2027

Our Enhanced BYOT Approach

St Peters operates an Enhanced BYOT model, where device requirements are tailored to suit different age groups. All secondary students are required to bring a laptop (Mac or Windows) to school each day. This model means that while families provide the student's device, the College provides a range of network, security and educational protections around its use at school.
When students are connected to the College network, these currently include:

- **Firewall filtering** to block adult content, gaming websites and servers, streaming services, known VPN services, and other categories of content that may be inappropriate or distracting in an educational environment;
- **DNS filtering** using Cloudflare Family DNS, providing an additional layer of protection against known adult and malicious content;
- **SafeSearch** enforcement across major search engines to help reduce exposure to inappropriate search results;
- **Network monitoring** to identify unusual traffic patterns and repeated attempts to access blocked content; and
- Ongoing identification and **blocking of VPN services**, proxies, and other emerging methods used to circumvent College network protections.

These protections are continually reviewed and enhanced as technology changes.

However, no school network or device model can provide an absolute technical barrier to inappropriate online activity. Personal hotspots, mobile data and increasingly sophisticated VPN technologies can potentially circumvent school network protections regardless of whether a device is family-owned or College-owned.

For this reason, our approach continues to combine strong technical controls, clear expectations for student behaviour, digital citizenship education, and partnership with families.

Should you have specific concerns about your child's device usage or would like guidance on home-based filtering solutions, please contact the College via our byot@stpeters.qld.edu.au email address.

Device Selection

In 2027 all students in Years 7-12 are required to bring a laptop to the College each day to support their learning. This booklet provides information and support for parents and students regarding this program.

The minimum specifications below serve as a guide for device selection. In 2027, all students in Years 7–12 are required to have a laptop or tablet computer with either a Windows or Mac operating system as their primary device. Both platforms are suitable for teaching and learning. When selecting a device, choose one designed to last at least three years.

Minimum Specifications for 2027

Specifications:

- CPU equivalent to or better than Ryzen 5, Intel Core 5 or Snapdragon X1 for Windows or M1/A18 for Mac
- Operating System: Latest version of Windows 11 or MacOS 27 (Golden Gate) or higher
- 8GB RAM (16GB or more recommended)
- 256GB SSD Hard Drive (512GB or more recommended)
- Minimum screen size 13”
- Minimum 7-hour battery life
- USB C port for charging and data transfer
- Audio port/Headphone jack

Mandatory requirement:

- Protective case and/or carry sleeve - Choose a durable and shock-absorbing case

Recommendations:

- Label or engrave equipment to ensure easy identification
- Investigate Accidental Damage Insurance (ADP) from the supplier or insurance provider
- Headphones - volume restricted over-ear headphones are ideal as they limit the maximum volume to a safe level which can be used for an extended period
- Additional laptop charger – to be stored in student lockers
- Mouse with scroll function - either Bluetooth or USB
- USB-C male to USB 3.0 female adapter (for computers without USB 3.0 ports)
- Stylus/Pen - for pen/touch enabled devices

Additional Information:

- An iPad Pro or Chromebook is not suitable for Years 7-12.
- If you are unsure if an existing laptop you already own is suitable, you can request advice via email to byot@stpeters.qld.edu.au.
- Please note that the College does not have preferred suppliers for purchasing your child's laptop. You may find it helpful to take this document with you when selecting a device.
- The College Insurance policy does not cover BYOT and personal devices. We take no responsibility for accidental damage to, or loss of student property. It is essential for parents to make their own arrangements regarding insurance and cover for accidental damage.

Required and Recommended Software

Information regarding the initial set up of a student's laptop will be provided through the BYOT Laptop Information page: https://stpeters.fireflycloud.net.au/byot/byo-laptop---years-7-12. New parents and students will be sent details with links to resources for set up before the academic year. Once you receive your child's account details, you are welcome to install the required software on their device. For further guidance on managing apps and settings, please see the *Recommendations for Parents/ Guardians* section of this document.

Software Requirements - Family Responsibility	
Web Browser(s) (students are advised to have more than one browser available in case of compatibility issues)	**Microsoft Edge is the preferred browser for St Peters.** Google Chrome and Safari (included in Mac OS) are also suitable as additional browsers if required.
Video Editor	Microsoft ClipChamp is included in the College's Microsoft 365 account or iMovie (Mac) or alternative video editing packages. ***Note:*** Microsoft ClipChamp, Adobe Rush or Premiere Pro do not need to be purchased as these are available through the College.

Software Requirements - College Provided	
Microsoft 365 (Microsoft Office)	**DO NOT PURCHASE Microsoft Office** as this software is provided to students. Instructions for set up will be provided on the BYOT Information Page.
Adobe Creative Cloud	**DO NOT PURCHASE Adobe Creative Cloud** as this software is provided to students. Instructions for set up will be provided as required.

Recommendations for Parents / Guardians

You are encouraged to consider the following to ensure the smart, safe, and responsible use of the laptop at home:

- Consider age-appropriate use of parental control tools or restrictions, such as:
    - Time-limiting or disabling access to some programs, websites or functionality.
    - Parent management of Apple ID or Microsoft account and installation of software or apps as is age-appropriate. Parents are advised to apply age settings to child accounts to prevent access to tools and settings that are not designed for specific age groups (eg. Under 13 years or under 18 years). This should also be set for accounts used to log in to web browsers such as Google Chrome (and related Google accounts) and Microsoft Edge.
    - With an administrator level account on your child's computer or management via a parent account on another device, it may be possible to restrict access to the AI tools that are embedded within the operating system of their device (such as Copilot, and Apple Intelligence/ Siri AI) or in browser (Gemini in a personal google account) in accordance with the terms of use for these tools.
    - Some parental control applications may require the use of a VPN, which can potentially conflict with College network settings. This conflict is less likely to occur when using parental control features that are integrated with or designed for the laptop's native operating system (Microsoft Family Safety and Apple Screen Time – see additional instructions below).
- At home, the laptop should be used in an open area, where it can be visually monitored.
- Invite your child to regularly show you what they have been doing and the tools they have been using.
- Respond with consequences if the device is not being used in an appropriate manner – some examples of consequences could be monitored use, restricted access, meeting with a teacher, or banning the use of the device at home for a period of time.
- Implement content filtering at home if you would like to control the content that can be accessed through the device.
- Ensure a balance of screen time and off-screen time as appropriate for your child's age.

Parents are encouraged to review all programs installed and apps their child requests, with attention to privacy, safety, and age restrictions. App and account use must comply with product terms, privacy policies, and age requirements, including for social media and Generative AI tools. From December 2025, new Australian legislation requires social media platforms to take reasonable steps to prevent users under 16 from creating or maintaining an account.

Setting restrictions via Microsoft Family Safety and Apple Screen Time*

Managing access via Microsoft Family Safety	Managing access via Apple ScreenTime
You can set up and manage Family Safety at https://account.microsoft.com/family/home Set your child's personal Microsoft account as a child of your parent / family organiser account. ***Settings*** • *Age Rating* can be used to restrict content, apps and games. • *Web Safety* allows options to reduce mature content. • *Ask to buy* enables approval for purchases from the Microsoft Store to install apps. • *Weekly email* sends a weekly report of use to your email • *Activity* can be sent to your email when clicked. ***Windows settings*** • Set Activity reporting to On. Regularly review your child's activity to inform family discussions and modify settings as appropriate. • Your child's device will appear as a connected Windows device when they first sign in. When listed choose the option to set time limits appropriate to your family circumstances and agreements. ***Website safety*** • In Filtering settings turn on the "Filter inappropriate websites and searches" option. This may be limited to Microsoft browsers only. • You may also want manage web access at a more detailed level by setting approved and blocked sites. However, this may reduce student ability to use online learning tools and content.	Set up family sharing on ***your*** Apple device. You can also set this on their MacBook by creating an account for yourself and then adding a child account via Settings. The latter does not give comprehensive management or alerts/ reporting of use. You will need to set a Screen Time Passcode. Do not share this code with your child. Ensure that ***your*** account (or another parent/ guardian) is a Family Organiser and that your child's age is specified. Apple provides a guide for parental control set up at https://support.apple.com/en-gb/guide/child-safety/kmp239668ukx/web **Screen Time Schedules** • Set time schedules and allowances for your child's laptop use. • Enable school hours to set restrictions for use of specific categories of apps within school days/hours. For example, pausing access to messages and social media during school. **Content and Privacy Restrictions** • There are default settings based on the age of your child. Content and apps can be blocked or allowed on their device. • If you set the "ask to browse" or "ask to buy" you may need to respond to requests promptly to support access to learning content at school. **Communication Restrictions** • You can set contacts to require approval for additional management. **Monitoring activity** • Regularly review your child's ScreenTime and device use to inform family discussions and modify settings as appropriate.

*The information on this page may not match current settings as Microsoft and Apple regularly update these.

Student Expectations

Students are expected to be ready to learn with their laptop by:

- Using the device responsibly, appropriately, and respectfully in accordance with the *Acceptable Use of Technology Agreement*
- Abiding by the College's *Academic, Assessment, Reporting and Honours Guide* to ensure academic integrity, especially regarding the use of Generative AI
- Using College WiFi only, no personal hotspots or VPN to bypass College restrictions
- Bringing their laptop charged, labelled and ready to use each day
- Ensuring the laptop is in its case/protective sleeve throughout the day to avoid physical damage
- Using their device as directed by teachers and within the appropriate areas and times specified by their sub-school
- Managing their time, use and the battery life of their laptop so that it can be used productively for educational purposes throughout the school day
- Locking the laptop in their locker when at sport or during activities not requiring the device, including at morning tea and lunch as specified for their sub-school
- Keeping passwords private and protecting their device so it requires a login when not in use
- Seeking permission before photographing, videoing or sharing online
- Maintaining the currency of the software and apps to ensure the tools for their learning are ready
- Backing up important work and files regularly (including the use of Cloud storage such as OneDrive)
- At all times being mindful of both their own digital reputation and that of the College

Consequences of misuse will be applied as deemed relevant to the behaviour and in accordance with sub-school behaviour management practices. These may include loss of internet privileges, restricted device use or other disciplinary action.

Technology and Wellbeing

The College adopts a range of approaches to ensure students, teachers, and the wider College community are equipped to embrace the potential of technology for learning, to contribute as responsible digital citizens, and to recognise and respond appropriately to online risks. St Peters students engage in a variety of learning activities designed to build their cyber-safety awareness, helping them to remain smart, safe, and responsible online.

The College filters access to the Internet, reducing the likelihood of students accidentally accessing undesirable sites. Use of the Internet via the St Peters wireless network is logged whilst students are at the College. Parents are encouraged to monitor their child's use of their laptop and other devices whilst at home, consider parental control tools, and filter their home Internet access.

The following Australian websites provide information and resources to assist in this endeavour:

- Tech and Wellbeing Firefly page stpeters.fireflycloud.net.au/tech-and-wellbeing (requires Firefly login)
- eSafety Commissioner www.esafety.gov.au
- Think U Know organisation www.thinkuknow.org.au
- Common Sense Media advice for parents www.commonsensemedia.org/advice-for-parents

Health and Safety When Using a Device

For good ergonomic practice, students are advised to consider the following when using their device:

- Take regular rest breaks within the confines of the classroom and as directed by your teacher
- Avoid using the device for more than an hour without a rest break
- Use the device on a desk rather than on the lap or floor whenever possible
- Angle the screen to minimise the need to bend the neck.
- Work in an environment free from glare and adjust the tilt of your screen to avoid reflections from lights or windows
- Maintain good posture and avoid sitting for long periods of time
- Increase font size for comfortable viewing
- When using headphones keep your volume low or use volume-restricted (to 89dB) over-ear headphones
- Keep screen brightness at a level that does not require eye strain and matches location of use

Contacts

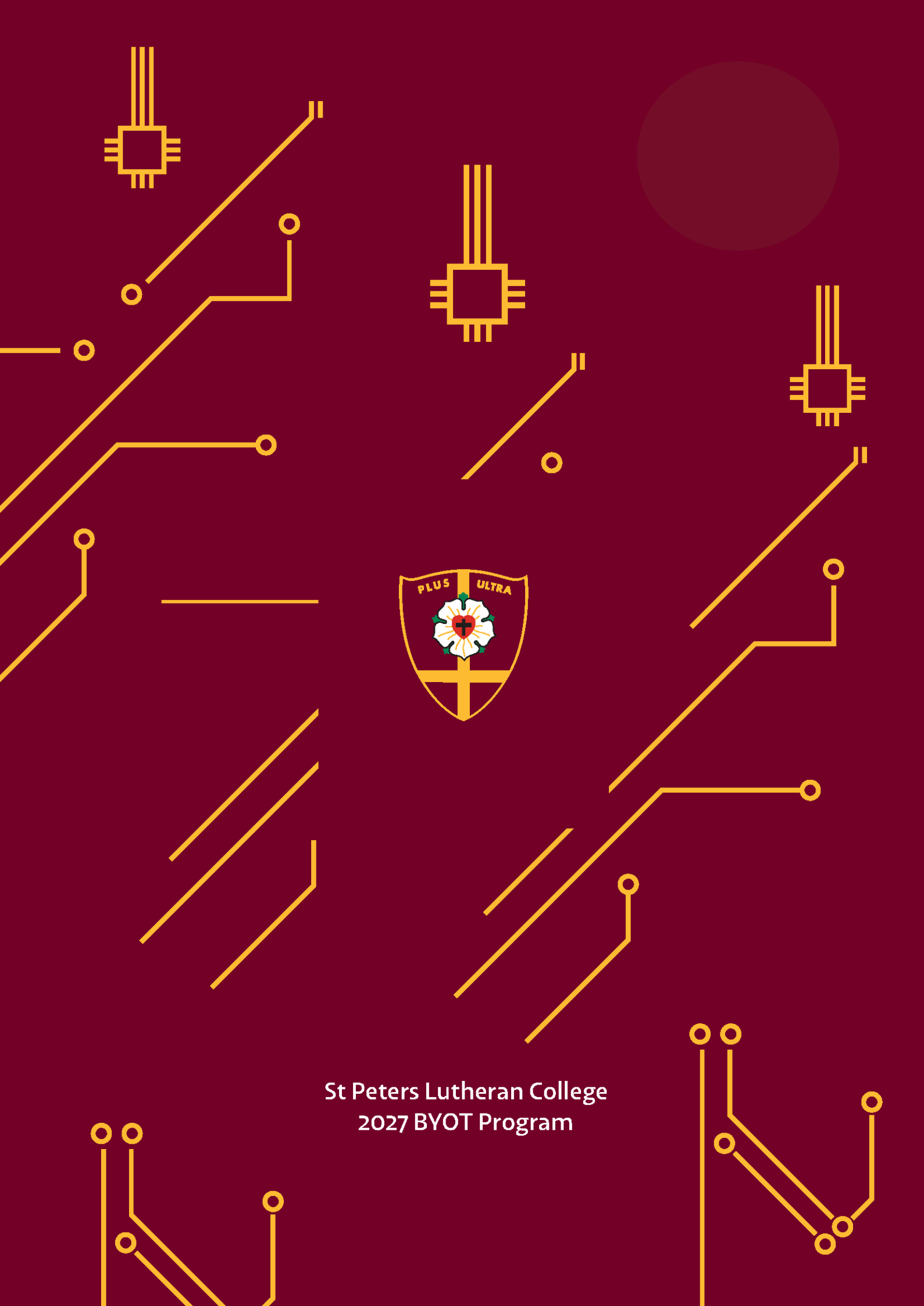
For queries regarding the BYOT program, please email byot@stpeters.qld.edu.au. More detailed information is available on the BYOT Information Page (http://stpeters.fireflycloud.net.au/byot).



Click to email a BYOT Query



Scan to view to BYOT Information Page



St Peters Lutheran College
2027 BYOT Program