Bring Your Own Device Policy & Procedures

Contents

Table of Contents

Purpose

This policy ensures that Sacred Heart International College (SHIC) supports student learning by outlining the rights and responsibilities of students for bringing, using and connecting their own devices to SHIC networks for coursework.

.

Definitions

Device: Laptop or Tablet (excluding mobile phones) brought by students, capable of connecting to SHIC's Wi-Fi network.

BYOD: Bring Your Own Device.

SHIC: Sacred Heart International College.

Bring Your Own Device Policy & Procedures

Policy

Key Principles

- **Definition of Device**

The term “device” in this policy refers to any personal mobile electronic device with the capability to connect to SHIC’s Wi-Fi network.

- **Internet Access**

Internet access will be provided through the wireless networks at no cost to students enrolled at SHIC.

- **Device Care and Maintenance**

Students are responsible for the care and maintenance of their devices, including data protection and battery charging.

- **Liability**

SHIC will not accept any liability for the theft, damage, or loss of any student’s device. Students bring their own devices onto the college site at their own risk.

- **Technical Support**

SHIC is not obliged to provide hardware or technical support for devices.

Purpose:

The purpose of the Bring Your Own Device (BYOD) Policy and Procedure is to provide guidance to staff and prospective students on the requirements and processes for the use of devices at Sacred Heart International College (SHIC). The BYOD program at SHIC aims to support student learning experiences by integrating technology throughout the educational program.

It will be compulsory for all students to bring, use, and connect their own devices to SHIC networks for use in their coursework at SHIC. This policy outlines guidelines for all stakeholders to understand and implement, so that everyone can become fully engaged in an exciting journey of exploring new frontiers in teaching and learning.

Implementation and Compliance

- Students must ensure their devices are adequately protected and maintained.
- SHIC reserves the right to restrict access to the wireless network if a device is found to be compromising the security or functionality of the network.
- Any misuse of the wireless network or breach of this policy may result in disciplinary action as per SHIC's policies.
- It is important to ensure that Students are aware of their obligations under this BYOD Policy and relevant Policies, prior to using their own Device on the SHIC Wi-Fi network. The BYOD Student responsibilities will be explained during Student orientation/induction session.

Information Dissemination

- This information is provided to students as part of the pre-enrolment process and is shared during orientation/induction sessions.

- It is essential that all students understand and agree to the BYOD policy before using their own devices on SHIC's Wi-Fi network.

Procedures

Student Responsibilities

- Students are solely responsible for the care and maintenance of their own devices.
- Devices should be used in the classroom as per Trainer's discretion, as the main purpose to use this Device in the classroom should be for education and study purpose.
- Students are responsible for managing the battery life of their device and acknowledge that SHIC is not responsible for charging their devices. Devices should be fully charged before being brought to class.
- Students are responsible for taking insurance coverage of their own devices to protect against accidental damage, theft, or loss.
- Students must have a supported operating system and current antivirus software installed on their device and must maintain the latest updates and antivirus definitions.
- Students should not attach any college-owned equipment to their devices without the permission of the trainer.
- Students are responsible for securing and protecting their devices. This includes using protective cases and common sense when storing the devices. SHIC is not required to provide designated or secure storage locations.
- Students are responsible for ensuring the operating system and all software on their devices are legally and appropriately licensed.
- When students are not using their device, they should store it in a classroom. Students are encouraged to take their devices home at the end of each day, regardless of whether they are needed. Laptops should not be stored in a vehicle as they can overheat or get stolen.
- Students are to ensure that they use their device in a responsible and ethical manner.
- Laptops must never be left in a backpack, unlocked car, or any unsupervised area.

Prohibited Student Activities

- Illegal installation or transmission of copyrighted materials.
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials.
- Accessing and using internet/app-based games within class time that are not deemed educational by the Trainer without prior permission.
- Use of messaging services within class time (e.g., Facebook/Twitter/Videos, Pictures and associated Apps) without prior permission from the Trainer or SHIC.
- Gaining access to another student's accounts, files, and/or data.
- Giving out personal information over the internet, including setting up internet accounts.
- Participation in fraudulent or other illegal behavior.
- Vandalism of personal, other students' or the school's technology (e.g., uploading or creating computer viruses).

- Participating in any form of bullying via social media.
- Presence of guns, weapons, pornographic materials, suggestive images, inappropriate language, alcohol, drugs, tobacco, and gang-related symbols or pictures.
- Using the SHIC network to seek out, access, store, or send offensive, obscene, pornographic, threatening, abusive, or defamatory material.
- Voice calling, text messaging, or instant messaging during class time.
- Taking photos or making video/audio recordings without permission from each individual being recorded and an appropriate staff member or Trainer.
- The CEO or Authorised Representative of SHIC determines appropriate use of BYOD devices within the bounds of Victoria privacy and other legislation.
- The consequences of policy breaches will be determined by the CEO or authorised representative, in accordance with SHIC policies.

Bring Your Own Device Policy & Procedures

Technology Standards

Student BYOD devices must meet the following technology standards for maximum efficiency of use at SHIC:

- **Web Browser:** Any modern web browser (e.g., Google Chrome, Mozilla Firefox, Microsoft Edge, Safari), with pop-up enabled.
- **Word Processor:** Microsoft Office Word 2016 or newer; alternatively, Google Docs or similar.
- **Presentation Software:** Microsoft Office PowerPoint 2016 or newer; alternatively, Google Slides or similar.
- **Wireless Compatibility:** Devices must have 2.4 GHz and 5 GHz range and allow through WPA Enterprise encryption of 802.11a/b/g or 802.11n.
- **Battery Life:** Ideal battery life of 10 hours, minimum of 8 hours.
- **Form Factor:** Laptop, Tablet, or Convertible Device
- **Physical Dimension:** Minimum screen size: 9.7", maximum screen size: 15.6".
- **Operating System:** Microsoft Windows 7, Windows 8.1 or newer; Apple MacOS X 10.8 or newer; Apple iOS 6 or newer.
- **Anti-Malware & Antivirus:** Device should be updated with antimalware and antivirus software.
- **Device Hardware Specifications:** Must meet the minimum (ideally the recommended) specifications of the operating system and all applications.

Course-Specific Specialised Software

For Accounting and Financial Services Courses (FNS40222, FNS50222, FNS60222): In addition to the general technology requirements listed above, students are expected to have Microsoft Excel for effective spreadsheet management. Depending on the specific units, students are also required to use industry-standard accounting software such as MYOB to complete tasks related to financial reporting, tax preparation, and bookkeeping.

For Information and Communication Technology Courses (ICT50220, ICT60220): In addition to the general technology requirements listed above, students require use of specialised software depending on the specific units within their course. Students use various tools like VMware or VirtualBox for virtualization, Cisco Packet Tracer for network management, and Wireshark for cybersecurity tasks. Security software such as Nord VPN, Avast Antivirus, and VeraCrypt is also essential. Project management and communication rely on tools like Slack, Trello, Asana, and Google Drive.

Students will be provided with instructions regarding specific course-related software by their trainers during class.

Bring Your Own Device Policy & Procedures

Borrowing Procedure

- In exceptional or emergency situations (compassionate and compelling circumstances), a limited number of laptops can be made available for SHIC students on a first-come, first-served basis.
- If a student needs to borrow a laptop at SHIC, they must check the availability at Reception and request to issue a laptop if one is available.
- The student must provide their Student ID card for the issuance of the laptop.
- The laptop issuing authority will scan the device for record maintenance purposes before issuing it to the student.
- Borrowed devices must be returned to SHIC Reception on the same day within college working hours.

Document Control

Document No. & Name:	Bring your own device P&P V2.1
Quality Area:	Students and Clients
Author:	Sanna Tayyib
Status:	Approved
Approved By:	CEO
Approval Date:	23 Aug 2024
Review Date:	23 Aug 2025
Standards (SRTOs):	Clause 1.3
Standards (National Code)::	Standard 11.2