Bring Your Own Device (BYOD)

Policy

Introduction

From Grade 4, students work with the "Bring Your Own Device" (BYOD) model, as a catalyst for teaching and learning processes in the classroom. This model means that each student brings their own electronic device to school to work on subject content, while the school deepens the collaborative use of content creation tools and accessibility for multiple resources and platforms from anywhere, at any time.

Students have personal lockers where they can safely store their personal belongings and leave their electronic devices.

About this Policy

We recognize that many of our students have personal electronic devices that they could use for learning purposes, and that there can be significant benefits for both students and teachers, including increased learning flexibility, in permitting such use. However, the use of personal devices for learning by students gives rise to increased risk in terms of the security of school IT resources and communication systems and the protection of confidential information.

Anyone covered by this policy may use a personal electronic device for learning purposes if they sign the declaration at the end of this policy and adhere to its terms.

This policy sets out the conditions through which a student may bring their own device into school to use for educational purposes.

Scope and Purpose of this Policy

This policy applies to students who use a personal electronic device including any accompanying software or hardware (referred to as a ***device*** in this policy) for learning purposes. It applies to use of the device during and outside school hours on the school site.

When you access school systems using a device, the school is exposed to risks, including the threat of malware (such as viruses, worms, spyware, Trojans, or other threats that could be introduced into our systems via a device). This could result in damage to school

systems. This policy protects school systems while enabling the students to access them using their personal devices.

This policy sets out the circumstances in which the school may monitor student use of school systems, access student devices and retrieve, remove, or destroy data on them and the action which the school may take in respect to any breach of this policy.

Some devices may not have the capability to connect to school systems. The school is not obliged to modify its systems or assist students in connecting to them should a device brought by the student not meet the outlined requirements and recommendations listed later in this policy.

Requirement & Recommendations for Devices

To ensure the correct device is purchased, we have outlined the following minimum requirements, recommendations, and security guidelines.

- In the event that a device is bought, we attach the following table with **minimum recommended requirements** that a device must meet in order to correctly perform educational tasks. Any device outside of these specifications must be tested, to confirm its correct functioning within the BYOD ecosystem in school premises.
- Computes with Windows **or** MacOS-based **operating systems** make it possible to integrate them into a BYOD ecosystem.

	GUY	WINDOWS	MAC	PURPOSE
HARDWARE	PROCESSOR	Intel i5 or higher	Intel i5, Apple M1 o superior	Increases speed and fluidity of the team
	HARD DISK	SSD 256 GB or higher	SSD 256 GB or higher	Increases speed and fluidity of the team
	RAM	8 GB or higher	8 GB or higher	It allows you to work simultaneously with different applications and processes.
	SCREEN	13" – 15"	13" – 15"	Good screen size-to-weight ratio team
	NET	WIFI b/g/n Recommendable Wifi AC	WIFI b/g/n Recommendable Wifi AC	Ensure the quality of your WIFI connection
	OTHER	Built-in microphone and camera	Built-in microphone and camera	Make use of educational tools like Teams
SOFTW ARE	OPERATING SYSTEM	Windows 10 or higher.	- MAC OS 12 (Monterrey) the upper	Better Performance, Greater Protection, Fewer Errors
	PDF READER	Acrobat Reader	Acrobat Reader	Read documents

				PDF Format
	VIDEO VIEWER	VLC	VLC	Watch videos own and others
	OFFICE AUTOMATION	Office 365	Office 365	Provided by the Institution. Integrated suite of applications and services.
	ANTIVIRUS	TrendMicro/ Microsoft Defender	Trend Micro/ Microsoft Defender	Provided by the Institution.

Protection

It is highly recommended that all devices should have the necessary protection to prevent any accidental damage that could occur to the screen, device, or any other components. The maintenance and repare of hardware is the sole responsibility of the family and student. It is recommended that suitable insurance or a warranty is purchased by the family to cover both school and home usage.

Security, Theft, or Damage

- BYOD devices and/or any peripheral hardware are the sole responsibility of the student.
- Students are responsible for the security of their device and any peripheral hardware. If placed into the provided locker, lockers should be locked and PIN code kept confidential.
- Teachers and other staff will not store or hold onto devices.
- IT staff and technicians will support and troubleshoot student devices or any peripheral hardware for everyday issues, but they will **not repair** or troubleshot beyond the most basic of ordinary level of support.

User Guidelines

- Devices should be fully charged at the beginning of the day.
- Devices should never be shared or lent to other students from New World International School or other school.
- A charging device will be brought to school every day to ensure that the device can be used throughout the school day.

Acceptable Use Agreement

Use of a BYOD whilst accessing the School Network in or out of school is in accordance to the Acceptable Use Agreement below. All students and parent or legal guardian are required to co-sign this agreement before access is granted.

Before use of your BYOD is permitted, this agreement must be signed and returned by the student and a parent or legal guardian.

Students should only access their specific WI-FI **Student Network**. They are not permitted to access others, like Guest or Staff Networks.

Social Media access is not permitted unless it forms part of a lesson, directed, and guided by a teacher.

1. Teachers may request, at any time, that BYOD devices are turned off in or out of the classroom. Failure to follow teacher instructions may result in restriction of School Network access and denial of school use.

2. Students should not attempt to log-in with the password of any other student or staff member.

3. All student passwords and log-in information are private and should not be shared with others.

4. In the future, the school may decide to install access limiting software on BYODs that restrict their use in the school network, including website access governance and limiting use of certain apps deemed not educational or part of school use.

Agreement NWIS BYOD Policy

Personal Technology Device Acceptable Use Agreement	
Parent Name:	Signature:
Student Name:	Signature:
Group:	
Date:	
Device Details: (optional to provide)	
Insurance/Warranty Details: (optional to provide)	