GEMS WELLINGTON INTERNATIONAL SCHOOL

BYOD Acceptable Use Policy Students

Reviewed by: <u>Abeda Natha</u>

Date of review: <u>June 2023</u>

Next date of review: <u>June 2024</u>

BYOD at WIS
At GEMS Wellington International School, the BYOD policy places a strong emphasis on the wellbeing of our students and the values of fortitude, empathy and integrity. We want students and parents to feel secure in the knowledge that this policy is designed not only to support but also guide safer working practices concerning the presence and use of devices within and around the school.

Students and parents/guardians participating in Bring Your Own Device must adhere to the Acceptable Usage Policy. Please read the information below:

Definition of "Device"

When "Device" in referenced in the Bring Your Own Device policy, it explicitly refers to electronic equipment, inclusive of tablets and laptops. These devices can connect to a network wirelessly, access the internet, and enable a wide range of applications and communication capabilities.

Network Access and Security

All students can register 1 personal device with the schools IT department to facilitate using them on the school network. Students must connect to the school's Wi-Fi network to ensure access is only to pre-approved websites and content. This registration supports in tracking incoming and outgoing traffic requests and ensures compliance and policy requirements. Such policy ensures undesired or unacceptable requests can be flagged with necessary measures taken. Devices must have password protection and/or biometric security features and it is desirable to have a suitable anti-virus software installed.

Acceptable Use

Device usage during school hours can be facilitated in classrooms during lessons with teacher supervision and direction. Such usage will be determined by the teacher, supporting the teaching and learning pedagogy. Non-educational activities, such as gaming and social media do not fall under acceptable usage.

Parental Responsibility

It is the parent's responsibility to oversee their child's usage of devices. This includes actively monitoring and engaging in online activities, establishing healthy choices regarding screen time, content restriction and ensuring access to age-appropriate websites or applications. Parental accountability is essential in helping student develop cognitive behaviour to develop responsible and safer digital habits.

Security and Damages

Responsibility to keep the device secure rests with the individual owner. The school is not liable for any device that is stolen or damaged on site. If a device is stolen or damaged, it will be handled through the administrative office similar to other personal artifacts that are impacted in similar situations. Additionally, protective cases and screen protectors for devices are strongly encouraged.

Responsible Digital Citizenship

Students must follow the school's acceptable usage policy and guidelines for responsible digital citizenship. This includes respecting copyright and intellectual property rights, refraining from cyberbullying or harassment, avoid sharing or revealing personal information, such as home addresses and personal telephone numbers. This also involves adhering to appropriate online etiquette. Where registration/log in is required, students should access all education sites and content using only the school provided @gemswis.com email address and not personal email addresses. Above guidelines are in line with the United Arab Emirates morals and culture etiquette.

B.Y.O.D. Student Agreement

The BYOD policy is a supplement to educational teaching and learning environments giving access to educational applications and online content, therefore failure to adhere to the school BYOD policy can result in temporary or permanent retraction of network or device access.

- Each student is responsible for the safekeeping and responsible use of their personal device and must ensure it remains in their possession at all times.
- Student's must take responsibility for the security measures on their personal devices, including password protection and antivirus software.
- Devices may not be used anywhere around the school or on buses without supervision or permission.
- Devices may not be used during assignments, unless students are otherwise instructed to do so, or for test or non-instructional purposes such as making personal phone calls and text or instant messaging.
- Devices may not be used to record, transmit, or post photographic images or videos of individuals onsite during school activities and/or hours.
- Students may only access files on internet sites that are relevant to the classroom curriculum as instructed by a teacher.
- Students must ensure that private content, gallery images and media stored on their devices are not access or viewed during school time.
- Students are required to comply with teachers requests to shut down the computer or close the screen when directed.
- Students understand that bringing in viruses of any type onto the premises or infecting the network is strictly prohibited.
- Student understands that compromising the school network intentionally or unintentionally can result in disruption of service and the principal's intervention.
- With instruction from the principal, the school's IT department has the right to collect and examine any device that is suspected of being complicit in a threat to the school network.
- Students are responsible for ensuring devices are charged and ready for the school day, portable chargers or power banks can support this.

By bringing in their device, students understand and will abide by the above policy and guidelines. Students further understand that any violation may result in the loss of my network and/or laptop privileges as well as other disciplinary action.