# The Millennium School, Dubai

## Policy on BYOD

**Implemented** : April 2014

**Reviewed** : September 2021

**Next Review** : September 2022

**Compiled by** : EDU. SMT

**Approved by** : Ambika Gulati
Principal

---

**Signature**

## 1. Rationale

The Millennium School uses instructional technology as one way of enhancing our mission to impart skills, knowledge and dispositions that students will need as responsible citizens in the global community. Students learn collaboration, communication, creativity and critical thinking in a variety of ways throughout the school day. In an effort to increase access to those 21st Century skills, TMS will allow personal devices to be brought to school.

The Bring Your Own Device (BYOD) program, which encourages students to bring their devices on a regular basis to school, has been initiated ONLY for students who follow the responsibilities stated in this Policy.

## 2. Purpose

The purpose of this BYOD policy is to ensure that all students use technology at school, home and elsewhere effectively, safely and responsibly.

## 3. Coverage

- The Policy provides guidelines for using digital hardware and software on school and personal computers/devices, on local area networks, wide area networks, wireless networks, the Internet and other technological equipment such as printers, servers, Smart TVs, Projectors, etc. when students are at school.
- The policy also applies to students' use of all such devices outside of school.

## 4. School's responsibilities

The school is responsible for:

- Providing technological hardware/ software/ network access to promote teaching and learning within the school community.
- Maintaining the integrity, operation, and availability of its electronic systems for access and use.
- Providing a safe cyber environment for all users through firewalls and MDMs.

The school does not guarantee user privacy or system reliability.

## 5. User Rights & Responsibilities:

It is expected that all users of the network, digital resources will:

- Obey the laws and restrictions of the United Arab Emirates.
- Respect other users in the School community, which includes the **strict prohibition of cyberbullying and harassment**;
- Always use your own login account and password and not through any other individual's

- Do not disrupt, delete and tamper with someone else's work that is saved on school devices and network.
- Recognize and honour the intellectual property of others.
- Comply with legal restrictions regarding plagiarism, the use and citation of information resources and copyright law;
- Limit the use of the school's technology resources to the educational vision and mission of the school;
- Use non-curriculum relevant materials only in their own time, outside of school and without detriment to their studies;
- Help maintain the integrity of the school network and equipment;
- Avoid tampering or experimenting with the school network or equipment, including efforts to bypass the school's Internet filters or proxies or the MDM system;
- Make personal devices available for inspection by an administrator or other staff member upon request;
- Use appropriate language in all communications;
- Never use or attempt to use another student's assigned hardware, subscriptions, logins, files, or personal information;
- Avoid giving out personal information, such as name, address, photo, or other identifying information online, including username and password;
- Avoid using personal devices or equipment to record (audio/visual) others without their permission;
- Avoid modifying or copying any protected system files, system folders, or control panel files without prior approval of the School's IT Department; and
- Avoid installing any softwares that will compromise on the safety and security of the system such as VPNs.
- Use the internet for educational and administrative purposes only. Use of the internet for emails and social networking sites is for only educational needs.
- Inform the IT team before installing any softwares on the school devices
- Use only licensed software for educational purposes
- Handle devices with care and be responsible for any loss or damage to individual devices
- Report any problems with the equipment to the IT department

**6. Users are not expected to:**

- Store commercial software, music, games or any hidden files and folders on their devices
- Store parents' files and folders on their devices

- Play games in school
- Download unlicensed software
- Repair, reconfigure, modify or attach any external devices to existing hardware without the permission of the IT department

Infringement or violation of U.A.E or international copyright laws or restrictions will not be tolerated.

**7. Cyber-Bullying:**

This involves the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group that is intended to harm others.

Students will be held accountable for Cyber-Bullying, even if it occurs off-campus during the school year and negatively impacts the academic environment of The Millennium School. The Millennium School has a zero tolerance for Bullying, including Cyber-Bullying.

**8. Installation of Mobile Device Management**

- The School will install a MDM on all student's BYOD as well school provided devices.
- Each student is allowed to bring only ONE device for the entire academic year.
- The device will be configured by the school IT Team to install the MDM.

**9. Purpose of MDM**

The purpose of installing the MDM in student devices is that it will enhance the safety and security of the device while the students are in the school complex. It will also enhance the effective monitoring of devices that are brought to school.

It will also restrict the applications that students can access whilst at school. The MDM will block all applications that are not required for learning by the students. The MDM will not allow users to access the schools' shared resources.

**10. Use of device at home in which an MDM is installed**

Once a device goes out of the school network, all applications installed on the device will become functional.

**11. Hardware Specifications**

Only the following devices can be brought to school for the successful configuration of the MDM license.

| Manufacturer | Model | Type | OS Version | CPPM Version |
|---|---|---|---|---|
| Apple | Ipad Air 2 | Tablet | 8.x, 7.6, 6.x, 5.x, 4.x | 6.1/6.0.2/6.0.1/5.2 |
| Apple | Mac | | OSX 10.7 10.8 10.9 10.10*) | Requires 6.2.3Asus |
| ASUS | Tab | Tablet | Android 4 | |
| Samsung | Galaxy Note 3 | Tablet | Android 4.1.2 | [6.2][6.1] |
| Lenovo | Tab 3 | Tablet | Android 3 and above | |
| Dell | Streak | Tablet | Android 3.2 | |
| ASUS | Nexus 7 Tablet | Tablet | Android 4.2.2 | |
| Microsoft | Windows | Tablet | Windows 10.8 | |
| IBM | Lenovo T450s | PC | Windows 10.8 | |
| DELL | XPS 10 | Tablet | Windows 10.8 | |

**12. Uninstalling the MDM**

Students should not uninstall the MDM once the license is installed in their device. Should they uninstall the license, it will prevent their device from accessing the school internet.

**13. Change of Device during an academic year**

Device change during an Academic Year is only allowed under special circumstances with written request from parent. Any change of device needs to be reported to the supervisor, who will inform the IT Team and get the license transferred to the new device.

**14. Non- compliance with Policy**

It is expected that all users of the school network, technological devices and digital resources follow the guidelines mentioned in this policy at all times and anywhere in the school. Users risk the loss of digital privileges in case it is found that the guidelines are not being followed. In cases of serious breaches, further action may be taken, in line with the School's standard disciplinary procedures.

**15. Lost, Stolen, or Damaged Devices**

Each user is responsible for his/her own device and should use it responsibly and appropriately. TMS takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. While school employees will help students identify how to keep personal devices secure, students will have the final responsibility for securing their personal devices. Please check with your homeowner's policy regarding coverage of personal electronic devices, as many insurance policies can cover loss or damage.