مدرسة التفاحة العالمية
The Apple International School

BYOD (Bring Your Own Device) Policy

Table of Contents

1. RATIONALE

The focus of the BYOD program at The Apple international, Dubai is to provide tools and resources to the 21st Century Learner. Excellence in education requires that technology is seamlessly integrated throughout the educational program to empower students to maximize their full potential and to prepare them for further studies and the workplace.

The policies, procedures and information within this document apply to all kinds of devices mostly tablets that will be used at The Apple international, Dubai including any other device considered by the administration to come under this policy.

At school, the device will be used for supervised research works in the classroom, for spot evaluation of the classroom learning, to access the digital text contents, to use as a platform for school provided resources wherever applicable, to practice assessments, to do extension activities uploaded to the site by teachers, to complete questionnaires and surveys shared from school, etc. it also enables them to access their Class/Subject Teams, download teacher-made assignments, complete it in the prescribed time and upload the same with ease. Moreover, the device is also made use of to attend The International Benchmark Tests like CAT4, e-TIMSS, e-PISA, e-PIRLS & PASSME that are mandatory but conducted online by the government approved agencies in Dubai. Some of the school assessments are also conducted in the online platform through the device. Therefore, equipping your child with a suitable device is more than a necessity in the evolving digital environment.

2. INTENDED USE:

This BYOD Policy has been developed to educate the school's communities (Students, Staff, Parents and Administration) of the roles and responsibilities of maintaining a responsible, safe and effective BYOD program.

2.1 WHO DOES THIS POLICY APPLY TO?

This policy applies to all stakeholders in the school's BYOD Program including:

- Students;
- Staff;
- Parents/guardians; and
- Principal Administrators

2.3 WHAT DEVICE/S DOES THIS POLICY REFER TO?

For the purposes of this policy, the term 'devices' refers to the use of the tablets (iPads, iPad Mini and other Android/ Windows tablets).

3. IMPLEMENTATION:

3.1 CLASSES BEING INCLUDED IN THE BYOD PROGRAM

Classes from Grade 1 onwards will be part of the BYOD program:

1. All Year 1 to 4 students –

The IT team will register the devices for this Grades group and only registered devices will have access to the school's internet and online facilities. The device's IP will be bound to MAC and students are advised to bring the same device to school each time to avoid disruptions.

2. All Year 5 onwards students –
   The students can bring their devices and login to the school network using the login credentials provided by the IT team.

For families opting to not participate in the BYOD Program, the school will have some devices available which will provide student access to technology, however these devices may be shared with other students within the class.

3.2 MINIMUM DEVICE REQUIREMENTS

The device must:

- Screen Size - Any iPad or Android/ Windows tablets.
- Have enough storage to install the selected applications set prior to the commencement of the school year by the BYOD staff; 32GB minimum (64GB preferred)
- RAM 8GB minimum
- Battery Life - 4 hours +
- Be Wi-Fi capable 2.4/5Ghz supported (802.11a/b/g/n) -**The tablets should not contain SIM cards.**
- Ensure accidental damage is minimised through being secured in protective casing.
- Tablet device that can utilise the latest operation system (iOS/android etc.) and support the installation of the most recent applications.
- Accessories - Protective bag/case. Headphones during the external exams.

We encourage parents to organise the use of a later model device as these devices will ensure compatibility and supportability for a longer period. However, this is not a requirement of the program and if students only have access to an earlier model device, then the school will allow its use.

3.3 TECHNICAL SUPPORT

As part of the BYOD Program, the school will offer a limited technical support program that will assist in helping students with:

- Connecting to the school's network and internet;
- Installing applications.

Due to the device being owned by the student and family, all other technical support and warranty issues will need to be sourced by the student's family from an external source.

3.4 ACCIDENTAL DAMAGE AND THEFT

The school does not provide accidental damage or theft cover for 3rd party (student-owned / teacher-owned) devices and shall therefore not be liable for any damages or theft that occurs on the school's premises unless:

- The device was under the direct care of a staff member.

3.5 ROLES, RESPONSIBILITIES AND GUIDELINES

STUDENT RESPONSIBILITIES

As part of the school's BYOD Program, students will ensure that they:

- Use their devices in a responsible and ethical manner;
- Their device is charged, has enough storage space and is kept in secure casing to enable daily use;
- Obey general school rules concerning behaviour and communication in line with the school's 'Code of Conduct';
- Protect their devices by contacting their teacher/administrator about any security problems they may encounter;
- Monitor activity on their accounts (e.g. MS Teams) and report any behaviour that is not in line with the school's 'Code of Conduct';
- Report any damages that may occur to their teacher immediately so that the teacher may investigate and inform the administration and parents of the child(ren) regarding the circumstances;
- Only update OS and applications over the school wi-fi in non-peak times (e.g. recess/lunch) once given permission by the school's ICT coordinator.
- Will use the internet in a safe and appropriate manner and will report any inappropriate or offensive websites to their teacher so that the administration can block those sites; and
- Respect and look after all devices, including their own, other students and the school's devices.

STUDENT ACTIVITIES STRICTLY PROHIBITED

- Illegal installation or transmission of copyrighted materials;
- Any action that violates the school's Code of Conduct or public law;
- Sending, accessing, uploading, downloading, or distributing offensive or explicit materials;
- Please note, the network will block all connections that are deemed inappropriate. This will include VPN connections. If there is a VPN on your device, ensure it is uninstalled while in School. The use of VPNs is prohibited in the UAE. This ensures that we can maintain a safe online environment for your child by filtering their online content through our Firewall and limit their risk of accessing inappropriate content.
- iPads/Tablet that have cellular connections must have this turned off and only connect online through the School Wi-Fi network.
- Accessing and using internet/app-based games within class time that are not deemed educational by the teacher without prior permission;
- Use of messaging services within school time (E.g. Facebook/Twitter) without the prior permission of the students' direct teacher;
- Gaining access to another students' accounts, files and/or data;
- Giving out personal information, for any reason, over the internet. This includes, but is not limited to, setting up internet accounts including those necessary for chat rooms, eBay, email, etc.
- Participation in fraudulent or other illegal behaviour;
- Vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that

can infiltrate computer systems and/or damage software components) of personal, other students or the school's range of technology;

- Participating in any form of bullying via social media (including, and not limited to texting, emailing, posting and accessing other student's devices); and
- Not using the School's web filter to access the internet at school.

STUDENT GUIDELINES

General Precautions

- The device is the student's property and should be treated with respect and care;
- Students are responsible for keeping their devices charged for school and
- Students must keep their device in protective casing at all times.

Device Identification

Student devices will be labelled by a manner specified by the school. Devices can be identified in the following ways:

- A record of the device's serial number and MAC address on the school's database (for year 1 to 4) and firewall records for grade 5 onwards;
- Clear labelling of the device and all accessories (Parent/Guardian Responsibility); and
- Installation of the Find My Device app.

Devices left in unsupervised areas

Under no circumstances should devices be left in unsupervised areas (including, but not limited to, school grounds, open building spaces, computer lab, specialist areas, library, offices, unlocked classrooms or toilets). Any device left in these areas is at risk of being stolen or damaged. If a device is found in an unsupervised area, it will be taken to the office. Violations of this section may result in loss of device privileges and/or other privileges.

Device Left at Home

If students leave their device at home, they are responsible for getting the course work completed as if they had their device present.

Charging Your device's Battery

Device must be brought to school each day in a fully charged condition. Students need to charge their device each evening. In cases where use of the device has caused batteries to become discharged, students may be able to connect their device to a power outlet in class at the teacher's discretion.

Sound, Music, pictures, Games or Programs

Sound must be muted at all times unless permission is obtained from the teacher. Students may bring headphones to use when a teacher deems it suitable. Music is allowed on the device and can be used at the discretion of the teacher. Music with explicit language is not permitted on the device at school and will need to be removed from the device at a teacher's request.
Internet games that are not deemed as educational content are not to be downloaded or played at school. If game apps are installed, it will be with the School staff approval.

Inappropriate media may not be used as a screensaver or background photo. Apps, Videos and photos must be suitable for audience. Presence of guns, weapons, suggestive images, inappropriate language, alcohol, drug, tobacco, and gang related symbols or pictures will result in removal of content and disciplinary actions.

Internet Access

Students will have a small internet quota that is refreshed on a monthly basis. This will cover internet browsing for research, required app use and other downloads permitted by staff and teachers. (OS updates are suitable at school during off-peak times only). All large downloads including game Apps, App updates, music and video need to be completed during off-peak times (recess and lunch) and approved by the ICT Coordinator.

Usage Charges:

The school is not responsible for any possible device charges to your account that might be incurred during approved school-related use.

Saving to the device/Backups

Students may save work to the applications on the device. It is also advised that students use OneDrive (internet storage) to back up the information on their device.
Students will hand in assignments as specified by the individual teacher. It is the student's responsibility to ensure that work is not lost due to mechanical failure or accidental deletion. Device malfunctions are not an acceptable excuse for not submitting work.

Network Connectivity

The School makes no guarantee that the network will be up and running 100% of the time. In the rare case that the network is down, the School will not be responsible for lost or missing data. Students will be allocated a monthly data limit to access the internet (this will not be large enough to download large applications or internet video). Only pre-configured, IT admin approved wireless network will be available for accessing the internet.

Inspection

Students may be selected at random to provide their device for inspection. Inappropriate content will be removed, students who refuse to remove inappropriate content will not have use of their device at school until it has been removed.

PARENT/GUARDIAN RESPONSIBILITIES

Parents/ Guardians are an important part of the school's BYOD program and can assist in ensuring the safety of our students is maintained. As part of this, we ask that all parents/ guardians:

- Talk to their children and establish standards and values that their child(ren) should follow when using their device and accessing the internet and applications at home. (The school advises that usage at home is always supervised);

- Understand that the child and parent hold full responsibility for the device and the School is not liable for any mistreatment, breakages, vandalism or loss of the device.
- Consider taking up accidental damage and theft insurance (offered by most retailers) to be covered in the unlikely case their child's device is damaged.
- Make sure the device is clearly labelled with their child's name and that they too, have also recorded the serial number of the device;
- Ensure that their student's device is synced/backed up and the required apps are installed on the device ready for educational use;
- Understand that students under the age of 13 may not take part in age-restricted social networking sites such as Facebook without the consent of a parent/guardian

SCHOOL RESPONSIBILITIES

The school provides the foundation of the BYOD Program and has an essential role in ensuring not only educational value, but also social responsibility and safety is developed by its students. As part of the program the School will:

- Provide taught students access to internet and an office 365 email account which will provide them access to a standard suite of licensed software applications and the licensed office 365 suites that includes (some or all) and is not restricted to the following features. Office Suite (Word, Excel, PowerPoint, Outlook, OneNote, Microsoft Teams)
- Ensure all staff are trained in using the device and are familiar with the processes pertaining to the BYOD Program;
- Train teachers of the BYOD program about cyber safety and to allow curriculum time for teachers to teach about being cybersafe to their students.
- Provide filtered internet access to its students and monitor student use in line with the school's Internet Usage Policy.
- Seek to block materials considered offensive, profane, threatening, pornographic, obscene, or sexually explicit.
- Provide some limited and lockable areas in which students may charge their device securely;
- Educate students, staff and parents on safety guidelines for duration of use, posture, rest periods, stretching, noise and other environmental hazards (as outlined by the Department of Education and Early Childhood Development)
- Ensure that staff will carefully select online content for students to use and at times allow students to create accounts to log on to appropriate educational resource sites with permission. E.g. LightSail, Arabic Reading, Oxford owl, Mathletics, specific apps, etcetera.

EVALUATION:

This policy will be reviewed annually to ensure relevant information is updated and maintained.

I understand and will abide by the above policy and guidelines. I further understand that any violation is unethical and may result in the loss of my network and/or device privileges as well as other disciplinary action. During the school year, additional rules regarding the use of personal devices may be added.

_____ _____

Name and Signature of Student _____ Date _____

Name and Signature of Parent Date

Ms. Jaya Menezes
Executive Principal

Enacted and enforced on: 1st January 2014

Reviewed annually

Late date of Review: 7th September 2022