مدرسة الإبداع العلمي الدولية
INTERNATIONAL SCHOOL OF CREATIVE SCIENCE

Beam
Bukhatir Education Advancement and Management International

Acceptable Usage Policy (AUP) of

"BRING YOUR OWN DEVICE" (BYOD)

مدرسة الإبداع العلمي الدولية
INTERNATIONAL SCHOOL OF CREATIVE SCIENCE

Beam
Bukhatir Education Advancement and Management International

Table of Contents

Mission :

The focus of the Bring Your Own Device (BYOD) policy at ISCS Muweilah is to provide tools and resources to the 21st Century Learner. Excellence in education requires that technology is seamlessly integrated throughout the educational program. In a bid to develop "future ready" leaders, we have identified the need for students to have regular access to carefully selected digital tools, which will support them on this journey. These tools can open the doors for transformational learning to take place and truly change the way we as educators deliver a lesson and in turn, how students learn. In the new normal, BYOD tends to be a necessity.

Bring Your Own Device at ISCS :

In light of the growing need for access to digital tools, students from Year 1 – 13 (2020-2021 academic year) are required to bring an IPAD to school, which meets the minimum specification (details below). This device will allow students to access a plethora of learning opportunities through a selection of pre-approved applications. Students will also receive other benefit from the Microsoft Office 365 package, access to the school's network and a device management system which will ensure their personal wellbeing remains a priority.

BYOD includes all *Mobile* devices including laptops and tablets, while not school property, also fall under the Acceptable Use Policy whilst on school property or whilst on school related activities. However, the school is **NOT** responsible for the repairs, loss or theft or any damage resulting from their use on school property or during school related activities. Improper use of BYOD will lead to immediate confiscation and denied access to the school Wi-Fi network. The devices will only be returned to the parents or legal guardians of the student owning the device after a meeting in light of the school defined Behaviour management policy.

Conditions for Use

General guidelines:

1. **All** students in Year 1 – 13 (2020-2021 academic year) must purchase a device.
2. The device must meet the specification outlined in this document.
3. Each student device will be enrolled into the Mobile Device Management Solution (MDM) utilized by the school. The device can only be used in lessons once this has been completed.
4. Students will be given access to the ISCS wireless network and therefore agree to and accept the terms of this school policy.
5. Student access to the ISCS wireless network will be regarded as a privilege and not an entitlement. Use of the wireless network will require students to comply with clear conditions and expectations.
6. Student use of the network will be monitored carefully by the IT team using the Mobile Device Management solution implemented by the school.
7. When explicitly permitted by a member of staff (and only when so permitted), a personal device may be used in lesson to support the lesson objectives.

8. The purpose of the device is to support the student in his or her learning journey. It is to be used as a tool to carry out tasks for academic purposes only, as assigned by the educator. Using the device for other reasons e.g. playing games, social networking sites or messaging, is **PROHOBITED**.
9. Students must **NOT** attempt to circumvent the school's network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security.
10. Students must **NOT** use such devices to record, transmit, or post any of the following: photos, audio, or video of any person(s) within school.
11. The school reserves the right to inspect and check any device if there is reason to believe that a student has violated school policy or has engaged in other misconduct whilst using the device.
12. Students will be advised to keep their device with them at all times. Devices should be brought to school every day, fully charged with all the stipulated accessories.
13. No charging of personal devices will be allowed on the school site, due to Health and Safety requirements regarding Portable Appliance Testing (PAT) guidelines.
14. Devices should be turned off if not in use during lessons. Devices should not be used during transit between lessons, break time or lunch time
15. During lessons:
16. Use of personal devices is at the discretion of teachers and staff. Students must **ONLY** use devices as permitted by their teacher.
17. Devices must **NOT** disrupt the class or learning in any way.

Independent study:

Students can use personal devices to carry out independent study if time has been allocated by the teacher. This may occur under the supervision of the teacher **ONLY**.

Classroom guidelines:

1. Devices should only be out in lessons, with the explicit permission of the teacher.-
2. Students cannot use their device for playing games, watching videos, accessing social media or any activity which is not solely for the purpose of meeting the objective of the lesson
3. Students may be asked, at any time, to evidence their learning using their device if infringement of school policy is suspected- 3
4. If a device is hidden (e.g. messaging under the table etc.) staff will assume it is inappropriate use and take action according to the behaviour policy outlined below.
5. Filming or taking photos requires authorisation by the Head of section.
6. If a student should receive or see anything inappropriate on their device, they should speak to a teacher so the appropriate action can be taken
7. If a student exits something on screen or moves the device away as a teacher approaches, the device can be confiscated.
8. If students are not using their device appropriately, or are off-task while using the device, a warning will be given and then sanctions will take effect following any further infringement (see below)

School Liability Statement

1. Students bring their devices to use at ISCS at their own risk. Students are expected to act responsibly with regards to their own device, keeping it up to date, charged and ready for learning to take place. It is their duty to be responsible for the upkeep and protection of their devices. **ISCS is NOT responsible for**

    a. **personal devices that are broken while at school or during school-sponsored activities**

    b. **personal devices that are lost or stolen at school or during school-sponsored activities**
2. Any damage or disruption to the school network caused as a result of improper use of a student-owned device will be regarded as a very serious misconduct.
3. Students must keep their devices in a secure place when not in use (e.g. a locked locker or bag).

AUP/BYOD User Pledge

This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the User Terms and Conditions named in this policy, privileges will be terminated, access to the school's technology resources will be denied, BYOD devices will be denied access to the school's network and Wi-Fi facilities and the appropriate disciplinary action shall be applied. The School code of conduct/ behaviour policy shall be applied to student infractions.

Parent/Guardian Responsibilities

Parents have a responsibility to talk to their children about values and the standards that their children should follow reg arding the use of the Internet as they would in relation to the use of all media information sources such as television, tel ephones, movies, radio and social media.

School Responsibilities

- Provide Internet and Email access to its students.
- Provide Internet Blocking of inappropriate materials where possible.
- Provide data storage areas. (Microsoft Office 365)
- The school reserves the right to review, monitors, and restrict information stored on or transmitted via BYOD device s and to investigate inappropriate use of resources.
- Provide staff guidance to aid students in doing research and help assure student compliance of the acceptable use policy

Student responsibilities

- Using computers/mobile devices in a responsible and ethical manner.
- Obeying general school rules concerning behaviour and communication that apply to Technology equipment use.
- Using all technology resources in an appropriate manner so as to not damage school equipment.

- Helping the school protect our computer system/network by contacting the IT Help team about any security problems they may encounter through their supervisor.
- Monitoring all activity on their account(s).
- Students should always turn off and secure the devices after they are done working to protect their work and inform ation.
- If a student should receive an email containing inappropriate or abusive language or if the subject matter is questionable, he/she is asked to print a copy and turn it in to the IT Team/Head of Section.
- Ensuring all BYOD devices are fully charged at the start of the school day.
- Their BYOD device is brought to school each day, fully charged unless otherwise informed.
- Ensure their BYOD device has the Apps/software installed as requested by the school and maintain software upgrad es.
- Ensuring that anti-virus and anti-malware software is installed on the device and is kept updated regularly and frequently

Student Activities STRICTLY PROHIBITED :

- Not bringing the device for three days continuously.
- Illegal installation or transmission of copyrighted materials
- Students must **NOT** take pictures or movies of students .
- Any action that violates existing school policy or public law
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obsce ne, religious or sexually explicit materials
- Use of chat rooms, sites selling term papers, book reports and other forms of student work
- Internet/Computer Games without permission of the school.
- Downloading apps at school unless supervised by the teacher and parental consent.
- Spamming-Sending mass or inappropriate emails
- Gaining access to other student's accounts, files, and/or data
- Use of the school's internet/Email accounts for financial or commercial gain or for any illegal activity
- Use of Social Media/Instant Messaging such as MSN Messenger, Yahoo Messenger, WhatsApp, Facebook, Instagram, SnapChat
- Students are not allowed to give 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 credit card fraud, electronic forgery or other forms of 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 dama ge software components) of school equipment will be PROHIBITED
- Bypassing the School web filter through a web proxy, or use of VPN.
- Carrying a device with own internet data.

Consequences for Device Misuse/ Disruption to Learning

Minor Behavioural Offences				
Offenses	**Upon committing it**	**First repetition**	**Second repetition**	**Third repetition**
1. Not bringing the device for three days continuously. 2. Internet/Computer Games without permission of the school. 3. Downloading apps at scho ol unless supervised by the teacher and parental consent.	*Verbal warning *Document offence.	*Document offence. *Inform the parent/ guardian in writing. *Written warning.	*Deduct 2 points from the behaviour marks (parent/guardian informed). *Refer student to social worker. *Call the parent/guardian. *Undertaking to not repeat offence signed by parent/guardian. *Written warning for student and parent/guardian if no response.	*SMART learning team meeting. *Deduct 4 points from the behaviour marks. *Case study by the social worker. *Implement a set of strategies to reduce negative behaviour. *Convert the offences to the second degree if repeated again.
Medium Severity Behavioural Offences				
Offenses	**Upon committing it**	**First repetition**	**Second repetition**	**Third repetition**
1. Spamming- Sending mass or inapprop riate emails 2. Use of Social Media/Instant Messaging such as MSN Messenger, Yahoo Mess enger, WhatApp, Facebook, Instagram, SnapChat. 3. Carrying a device with own internet data.	*Call the parent/guardian and agreement for reforming child's behaviour to be signed. *Written warning. *Case study by social worker. *Deduct 4 points from the behaviour marks. *Monitor behaviour.	*Deduct 8 points from the behaviour mark. *Get the signatures of the parent/guardian and the student on a warning.	*Suspend the student for a max. of 2 days from the online learning platform and assign duties. *Written warning. *SMART learning team meeting. *Implement a set of strategies to reduce negative behavior. *Deduct 8 points from the behavior marks.	*Suspend the student from 1 to 3 days in the online learning platform and assign duties. *Case study by the social worker. *SMART learning team meeting. *Issue final written warning. *Deduct 8 points from the behaviour marks. *Convert the offences to the third degree if repeated again.

Serious Behavioural Offences		
Offenses	Upon committing it	First repetition
1. Illegal installation or transmission of copyrighted materials. 2. Students must not take pictures or movies of students. 3. Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornograph ic, obscene, religious or sexually explicit materials.	Upon committing: *Immediate convening of the Smart Learning Team to reach a decision.	First repetition: *Suspension from online learning platform immediately.

4. Use of chat rooms, sites selling term papers, book reports and other forms of student. 5. Gaining access to other student's accounts, files, and/or data. 6. Use of the school's internet/Email accounts for financial or commercial gain or for any illegal activity. 7. Participation in credit card fraud, electronic forgery or other forms of illegal behaviour. 8. Vandalism (any malicious attempt to harm or destroy hard ware, 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 school equipment will n ot be allowed . 9. Bypassing the School web filter through a web proxy ,or use of VPN.	*An immediate summons of the parent/guardian and signing of the decision and warning. *Deduct 12 points from the behaviour marks. *Deciding to refer student to behaviour modification centre. *Suspension from online learning platform immediately.	*Immediate convening of the Smart Learning Team to conclude a decision. *An immediate summon of the parent/guardian and signing the decision. *Deduct 12 points from the behaviour marks.

Device Specification

The digital strategy developed by ISCS is based on an internationally recognized model tailored to align with our values. In order for the successful implementation of our strategy, students must ensure that their device is in line with the specifications outlined below:

Student Year (2020-2021)	Device Type Option 1	Device Type Option 2
Grade 1 - 6 (Year 2 – 7) Primary School	Apple iPad 7th Generation (2019) 32GB WIFI only **Preferred**	**Windows 10 Laptop/Tablet**
Grade 7 - 13 (Year 8 – 13) Secondary School	Apple iPad 7th Generation (2019) 32GB WIFI only	**Windows 10 Laptop/Tablet**