مدرسة الإبداع العلمي الدولية
INTERNATIONAL SCHOOL OF CREATIVE SCIENCE
BAHRAIN | البحرين



Bring Your Own Device (BYOD) Policy

Bring Your Own Device Policy

Document Information			
Created by:	Head of IT Group Assistant IT Manager Principal	Reviewed by:	Head of IT Group Assistant IT Manager Principal
Review Cycle:	Annual	Next Review:	**March 2027**
Head of IT Group: Mohamed Sadawy Assistant IT Manager: Infrastructure & Cloud Services I IT: Mohammed Aijazuddin Principal: Ahmed Nadhim Al-Talib			

Contents

Mission 3
BYOD Guidelines 3
Conditions for Use 3
General Guidelines 3
During Lessons 4
Classroom Guidelines 4
School Liability Statement 5
AUP/BYOD User Pledge 5
Parent/Guardian Responsibilities 5
School Responsibilities 5
Student Responsibilities 5
Student Activities STRICTLY PROHIBITED 6
Consequences for Device Misuse 6
Minor Behavioural Offences 6
Medium Severity Behavioural Offences 7
Serious Behavioural Offences 7

Mission

The primary objective of the Bring Your Own Device (BYOD) policy at ISCS Bahrain is to equip our students with the necessary tools and resources to excel as 21st-century learners. In our commitment to delivering excellence in education, we recognize the indispensable role of technology in seamlessly integrating with our educational framework. With a vision to foster the development of "future-ready" leaders, we acknowledge the imperative for students to have consistent access to carefully curated digital tools. These tools serve to facilitate transformative learning experiences, reshaping the dynamics of both teaching and learning. In the contemporary educational landscape, BYOD has become not just advantageous but essential.

BYOD Guidelines

Acknowledging the increasing demand for access to digital resources, students from Year 2 to Year 6 are mandated to bring an iPad to school. The specifications for these devices are outlined below. These iPads will enable students to leverage a wide array of educational opportunities offered through pre-approved applications. Additionally, students will benefit from access to the Microsoft Office 365 suite, connectivity to the school's network, and a device management system designed to prioritize their personal well-being.

BYOD encompasses all mobile devices, including laptops and tablets. While these devices are not school property, they are subject to our Acceptable Use Policy while on school premises or engaged in school-related activities. However, it's important to note that the school bears no responsibility for repairs, loss, theft, or any resulting damages incurred while these devices are used on school property or during school-related activities. Misuse of BYOD will result in immediate confiscation and revocation of access to the school's Wi-Fi network. Devices will only be returned to the parents or legal guardians of the respective student after a meeting, in accordance with the school's Behaviour Management Policy.

Conditions for Use

General Guidelines

1. Students are not required to bring their devices to school daily.
2. Devices should be utilized to enhance learning for specific purposes.
3. Devices should not be used when traditional methods are more effective for learning.
4. The weekly schedule will specify the lesson, day, and focus for device usage if required.
5. Parents and students are responsible for ensuring that if a learning activity necessitates device usage, the device is brought to school fully charged, as indicated in the weekly schedule.
6. Devices must remain in student bags until the lesson where they are required.
7. Devices are not to be used during break time or while on the bus.
8. All students from Year 1 to Year 13 (academic year 2020-2021) must procure a device meeting the specified requirements.
9. Each student's device must adhere to the specifications outlined in this policy.
10. Student devices must be enrolled in the Mobile Device Management Solution (MDM) utilized by the school before being used in lessons.
11. Students will be granted access to the ISCS wireless network and must agree to abide by the terms of this school policy.

12. Access to the ISCS wireless network is a privilege, not an entitlement, and students must comply with clear conditions and expectations for its use.
13. Student network usage will be closely monitored by the IT team using the Mobile Device Management solution.
14. Personal devices may only be used in lessons to support lesson objectives with explicit permission from a staff member.
15. The purpose of device usage is to support students in their learning journey, restricted to academic tasks assigned by educators. Using devices for non-academic purposes, such as gaming or social networking, is strictly prohibited.
16. Students must not attempt to circumvent the school's network security or filtering policies, including setting up proxies or downloading programs to bypass security measures.
17. Recording, transmitting, or posting photos, audio, or videos of any person(s) within the school is prohibited.
18. The school reserves the right to inspect and check any device suspected of violating school policy or engaging in misconduct.
19. Students are advised to keep their devices with them at all times, ensuring they are brought to school daily, fully charged, and equipped with all stipulated accessories.

In terms of charging personal devices, no charging will be permitted on the school premises due to Health and Safety guidelines regarding Portable Appliance Testing (PAT). Devices should be turned off when not in use during lessons and should not be utilized during transitions between lessons, break times, or lunch.

During Lessons

The use of personal devices is at the discretion of teachers and staff, and students must only use devices as permitted by their teachers. Devices must not disrupt the class or learning in any manner.
Independent Study: Students may use personal devices for independent study only when allocated time by the teacher, and such usage must be supervised.

Classroom Guidelines

1. Devices should only be used in lessons with explicit permission from the teacher.
2. Devices must not be used for activities unrelated to the lesson's objectives, such as gaming, watching videos, or accessing social media.
3. Students may be asked at any time to demonstrate their learning using their device if there are suspicions of policy infringement.
4. Concealing a device (e.g., messaging under the table) will be assumed as inappropriate use and dealt with according to the behavior policy.
5. Filming or taking photos requires authorization from the Head of Section.
6. If students encounter inappropriate content on their device, they should report it to a teacher for appropriate action.
7. Attempts to conceal or minimize device usage upon a teacher's approach may result in confiscation.
8. Students failing to use devices appropriately or being off-task while using them will receive warnings and subsequent sanctions for further infringements.

1. Students use their devices at ISCS at their own risk and are expected to handle them responsibly, keeping them up-to-date, charged, and ready for learning. Students are responsible for the maintenance and protection of their devices. a. ISCS bears no responsibility for personal devices damaged, lost, or stolen on school premises or during school-sponsored activities.
2. Damage or disruption to the school network resulting from improper use of student-owned devices will be considered serious misconduct.
3. Students must secure their devices when not in use (e.g., in a locked locker or bag).

AUP/BYOD User Pledge

This policy serves to inform all users of their responsibilities concerning the efficient, ethical, and lawful use of technology resources. Violations of the User Terms and Conditions outlined in this policy will result in the termination of privileges, denial of access to the school's technology resources, exclusion of BYOD devices from the school's network and Wi-Fi facilities, and appropriate disciplinary action in accordance with the School's code of conduct/behavior policy.

Parent/Guardian Responsibilities

Parents are responsible for discussing with their children the values and standards guiding the use of the Internet, as they would with other media sources such as television, telephones, movies, and social media.

School Responsibilities

- Provide Internet and Email access to students.
- Implement Internet blocking of inappropriate materials where feasible.
- Offer data storage areas (Microsoft Office 365).
- The school reserves the right to review, monitor, and restrict information stored on or transmitted via BYOD devices, as well as investigate inappropriate resource use.
- Provide staff guidance to support student research and ensure compliance with the acceptable use policy.

Student Responsibilities

- Use computers/mobile devices responsibly and ethically.
- Adhere to general school rules regarding behavior and communication applicable to technology equipment use.
- Utilize all technology resources appropriately.
- Assist the school in protecting our computer system/network by promptly reporting any security issues encountered to the IT Help team through their supervisor.
- Students are responsible for monitoring all activity on their accounts.
- After completing work, students should always turn off and secure their devices to safeguard their work and personal information.
- If a student receives an email containing inappropriate or abusive language, or if the subject matter is questionable, they are required to print a copy and submit it to the IT Team/Head of Section.
- Ensure all BYOD devices are fully charged at the beginning of each school day.

- BYOD devices must be brought to school daily, fully charged, unless otherwise instructed.
- Ensure that BYOD devices have the necessary apps/software installed as requested by the school and keep them updated with software upgrades.
- Ensure that anti-virus and anti-malware software is installed on the device and regularly updated.

Student Activities STRICTLY PROHIBITED

- Failure to bring the device for three consecutive days.
- Illegal installation or transmission of copyrighted materials.
- Taking pictures or videos of students is strictly prohibited.
- Any action that violates existing school policy or public law.
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, religious, or sexually explicit materials.
- Use of chat rooms, sites selling term papers, book reports, or other forms of student work.
- Internet/computer games without permission from the school.
- Downloading apps at school without supervision by a teacher and parental consent.
- Sending mass or inappropriate emails (spamming).
- Attempting to gain access to other students' accounts, files, or data.
- Use of the school's internet/email accounts for financial gain, commercial activities, or any illegal activities.
- Use of social media/instant messaging platforms such as MSN Messenger, Yahoo Messenger, WhatsApp, Facebook, Instagram, or Snapchat.
- Students are prohibited from sharing personal information over the Internet, including setting up internet accounts for chat rooms, eBay, email, etc.
- Participation in credit card fraud, electronic forgery, or any other forms of illegal behavior.
- Vandalism of school equipment, including any attempt to harm or destroy hardware, software, or data, such as uploading or creating computer viruses or programs that can damage computer systems or software components, is strictly prohibited.
- Bypassing the school web filter through a web proxy or the use of VPN.
- Bringing a device with its own internet data.

Consequences for Device Misuse

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 school unless supervised	*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	*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.

by the teacher and parental consent.			offence signed by parent/guardian. *Written warning for student and parent/guardian if no response.	*Convert the offences to the second degree if repeated.
Medium Severity Behavioural Offences				
Offenses	**Upon committing it**	**First repetition**	**Second repetition**	**Third repetition**
1. Spamming- Sending mass or inappropriate emails 2. Use of Social Media/Instant Messaging such as MSN Messenger, Yahoo Messenger, 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, pornographic, 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.