



# BYOD - Bring Your Own Device Policy

## GRADE VI-XII

DPS Monarch International School is committed to aiding students in creating a learning environment where students develop the skills, dispositions, and behaviors necessary for responsible citizenship in a global community.

DPS Monarch International School has developed this BYOD (Bring Your Own Device) policy to provide opportunities to all the students to utilize various platforms as well as resources to extend and enrich learning through -

- Digital assessments (Concept Recap)
- Research for project work and ICT
- CISCO Educational Courses offered by CISCO.
- Engaging student-centered e-learnings where inquiry and authentic learning are emphasized.
- Using online learning tools and digital content.

The students of the Secondary and Senior Secondary School levels from Grade 6 to Grade 12 may use their privately-owned internet-enabled device on the school's wireless network subject to teacher and staff permission.

By giving permission, parents acknowledge adherence to all the schools' policies concerning the internet and social network usage, including the IT – Internet Policies, Social Media Policies, and Behavior Policies of School published on the website.

BYOD refers to any personally owned internet-enabled device used to complete assignments, projects, and other work. These devices include (laptops, tablets, iPads, Chromebook, MacBook) only, all types of mobile phones and other devices, and any other technologies are strictly prohibited to be used inside the school campus without prior permission from the school authorities.

**The use of personally owned Wi-Fi devices on Monarch School Networks is a privilege, not a right.**

Anyone connecting and using their personal devices to the DPS Monarch School BYOD are required to acknowledge receipt and understanding of BYOD Policy and is subjected to abide by its terms, conditions, and consequences. This policy is in line with the school's other policies and statements related to the use of the internet policies and other IT Policies. All users of the school's networks are bound by the fair use of internet provision and must agree not to abuse or overuse available internet capacity. If school found any over usage of internet, The school authority has rights to take necessary actions on immediate basis,

## **Important Guidelines -**

### **While using your own Device**

For an individual to bring and use his/her personal device at DPS Monarch International School as per school policy including the BYOD policy must be understood, agreed to, and adhered by:

- Charging locations at school are extremely limited and students are not supposed to charge their devices at school. Fully charged devices to be carried by the students them to school and should be able to run off battery power while being used throughout the day.
- Personally owned devices are not allowed to be connected directly to the school's wired network permission. Misuse of this provision will result in severe consequences.
- All devices used on the school networks must have an up-to-date anti-virus/ anti-malware program installed and enabled at all times. School is not responsible for damage or data loss caused by malicious programs accessed through the school networks.
- Each teacher has the discretion to allow and to regulate the use of personal devices in the classroom by the students and on specific projects.. Students must comply with the teacher's decisions on the use of the devices. While in class, personal devices may not be used for non- instructional purposes (making personal phone calls, text messaging, etc.)
- The device volume should be off or on silent mode when students are at School, unless otherwise authorized by the teacher, so as not to disturb others.
- Students, parents/ guardians, and other users acknowledge that School Internet access and information gathered while using it will go through the school's content filters which may not be bypassed. Students may only use their devices to access files on internet sites which are relevant to classroom assignments, activities, and the curriculum. Some sites, like social media are blocked by School firewall.
- To show respect for the rights of others, and to follow the school privacy policy, students may not use devices to record, transmit, or post photographic images, audio or video or reference to a person or persons (students, teachers, staff, etc.) on school property or during school activities without the consent of the person/ persons or otherwise allowed by a teacher. Devices must not be used to transmit content of a bullying nature or that violate local laws at any time.
- Games through devices are not permitted to play inside the school campus, it's strictly prohibited.
- Access to school printers from the BYOD is not permitted and not allowed to connect.
- Infecting any school property with any virus, Trojan, or malware or the use of a program that damages, alters, destroys, or provides access to unauthorized data/information is considered a serious violation. This includes bypassing network security provisions.

- The BYOD network is accessible only through Wi-fi.
- Students are not allowed to load apps on their devices without the knowledge of school authority. While connected to the school network, students may only download apps for classroom use if recommended by school.
- Students must not share passwords, use others' passwords, access others' accounts, or attempt to work around the school filter, network, or Internet. Students are advised not to lend their devices to others.

### **Unsupervised Areas**

- under no circumstances devices to be left in an unsupervised area. Unsupervised areas include the school grounds, campus, the lunchroom, Ground, computer labs, locker rooms, library, unlocked classrooms, dressing rooms, lobbies, and hallways. Any devices left in these areas is in danger of being stolen. If devices are found in an unsupervised area, it will be taken to the School Safety & Security Department. Students may face disciplinary action for leaving an devices unattended

**Note:** Devices are brought to school at the students' and parents'/guardian's own risk. The individual owner is responsible for the security and safety of the device.

- Individuals are encouraged to utilize security methods to protect their devices. Students are suggested to put label on their personal devices with a symbol or icon for ready identification. In addition, place and enable secure user access passwords associated with the device, and not loan or allow anyone else to use their personal device at any time.
- DPS Monarch International School and its employees are not financially or legally responsible for loss or damage of any personally owned device brought to the school.
- DPS Monarch International School is not responsible for management, troubleshooting, technical support, or repair of personally owned devices.

### **File and Data Management**

Students are responsible for managing the data by their own devices and ensuring that everything is backed up regularly.

Students may save files on the devices. As a safety precaution, students are encouraged to email important documents to themselves or use an online storage option (e.g. One Drive).

Data Loss due to Network Connectivity, 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.

## **Consequences/ Legal Propriety**

Students must comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity. If you are unsure, ask a teacher / parent / IT Department.

The use or possession of hacking software is strictly prohibited, and violators will be subjected to School Code of Conduct. Violation of applicable state or federal law will result in criminal prosecution or disciplinary action by the school.

Violation of DPS Monarch International School rules and use policies for internet access can result in a loss of access privileges, a prohibition of the use of the student's device within school campus, detention, and even suspension or expulsion, if the violation warrants.