SHARJAH INDIAN SCHOOL

Tel: 06 5670560 / Tel: 06 5671866
Fax: 06 5672914 / Fax: 06 5675166
P.O. Box – 2324, Sharjah
e-mail: mail@sissharjah.com Website: www.sissharjah.com

OUR VISION
Educate Enlighten Empower

BYOD POLICY

SHARJAH INDIAN SCHOOL

BYOD POLICIES AND GUIDELINES

In today's digital era, the concept of BYOD—Bring Your Own Device—is becoming increasingly prevalent in educational settings. This policy allows students to bring their personal devices, such as smartphones, tablets, and laptops, into the classroom to use as learning tools. BYOD in schools leverages the technology that students are already familiar with, potentially enhancing engagement and accessibility to educational resources. This introduction to BYOD will explore how this model operates within the classroom, highlighting the dynamic interaction between students' personal devices and educational systems, and discussing the overarching impact on teaching and learning processes.

Advantages of BYOD in Schools

- **Increased Engagement:** When students use their own devices, they are often more engaged in the learning process. Familiarity with their personal devices makes it easier for them to access educational tools and participate actively in lessons.
- **Familiarity with Devices:** Students tend to be more comfortable and proficient with their own devices. This familiarity can lead to quicker completion of assignments and more effective communication in digital formats

What kind of educational activities will the personal devices be used for?

- Working in Microsoft office for various purposes such as producing documents, spreadsheets, and/or slide shows, email communication and collaboration amongst their peers and teachers.

- File storage and sharing: OneDrive and SharePoint for the purpose of collaboration and accessing resources.
- Accessing the online learning environment during class to support learning.
- Access to video and audio recordings to support learning (Only in accordance with the Acceptable User Contract).
- The device requirements for each class are as follows:

• Device Type:Laptops/ iPad or Android/Windows tablets (or a similar tablet device). • Exclusion: Smartphones are not permitted. Devices must not have eSIM/SIM cards installed. • Rationale: Aligned with the curriculum and • software • requirements for the specified grades.

Guidelines for Students

1. The student is fully responsible, at all times, for their personal laptop. School is not liable for any loss/damage/theft or any monetary charges that may occur while the student is using the device.
2. Approved devices must be in silent mode while on school campus, unless otherwise allowed by a teacher.
3. Students required to bring their own headphones. Headphones may be used with teacher permission.
4. Devices may not be used for non-instructional purposes (such as making

personal phone calls and text messaging).

5. Devices should be sufficiently charged before the start of school every day.
6. Students may not use devices to record, transmit, or post photographic images or video of a person or persons on campus during school hours or during school activities, unless otherwise allowed by a teacher.
7. Devices may only be used to access computer files on internet sites which are relevant to the classroom curriculum.
8. Students must ensure they have the latest software installed on their devices, relevant to the subject area.
9. It is the student's responsibility to maintain sufficient memory capacity on their device to enable its use for educational purpose.
10. Devices must have appropriate protection/cases allowing easy carrying of the devices.
11. Devices must have a secure login and password.
12. The school behaviour Policy is applied if students fail to adhere to these guidelines.
13. If reasonable belief exists that the student has violated the conditions of this agreement the student's device may be inspected and/or confiscated. Subsequent or additional disciplinary action involving misuse of technology may extend to loss of technology privileges or further action as determined by the Head of Secondary.
14. Students are expected to bring in their device each day on the assumption that the teacher may elect to use them for their lessons.

Students and Parents/Guardians acknowledge that:

1. The school's network filters will be applied to a devices' connection to the

internet and any attempt to bypass the network filters is prohibited.

2. School is authorised to collect any device that is suspected of breaching the BYOD policy, the data protection and information security policy for the suspected source of an attack or virus infection. If the device is locked or password protected the student concerned will be required to unlock the device at the request of authorised staff with a parent present.
3. All students involved in the BYOD program will supply their own devices and be responsible for its safety, whilst on the school premises.
4. Students, Staff and Parents/Guardians are prohibited from knowingly bringing a device on premises that infects the network with a virus, Trojan, or programme designed to damage, alter, destroy, or provide access to unauthorised data or information.
5. Students, Staff and Parents/Guardians are prohibited from processing or accessing information on school property related to "hacking" altering or bypassing network security policies.
6. School is not responsible for restoring devices where passwords have been forgotten or the device is locked.
7. It is the choice of the individual families to insure devices against loss or damage.
8. Personal devices must be charged prior to school and run-on battery power while at school.
9. School is not responsible liable for loss or damage of student's personal devices or cases.
10. Any student in breach of this BYOD policy will result in the application of the School Behaviour Policy, possibly leading to confiscation of the device.

Prohibited Activities

The following activities are strictly prohibited

- Cyberbullying: Cyberbullying refers to any intentional, aggressive act carried out using electronic means, with the purpose of harming, harassing, or intimidating others within the school community. Engaging in any form of cyberbullying is strictly prohibited.
- Inappropriate Content: Accessing, downloading, or distributing inappropriate content, including but not limited to explicit material, hate speech, or violence, is not allowed.
- Hacking and Unauthorized Access: Attempting to hack into computer systems, networks, or unauthorized access to data is strictly prohibited. The UAE has stringent cybercrime laws, and unauthorized access to computer systems, hacking, and other cyber offenses are treated seriously.
- Copyright Violations: Students must respect copyright laws and refrain from unauthorized downloading, sharing, or distribution of copyrighted materials/software. The UAE has laws protecting intellectual property, and this extends to software. Unauthorized distribution or use of copyrighted software may be subject to legal action.
- Malicious Software: Intentionally introducing or spreading malicious software, viruses, or any form of malware is prohibited.
- Invasion of Privacy: Prohibits activities like photographing others without permission and handling electronic photos without consent,

underscoring the importance of respecting personal privacy.

- Defamation: Forbids the dissemination of news, photos, scenes, comments, or statements that, even if true, could harm an individual's or entity's reputation.
- Amending or Processing for Harmful Purposes: Restricts the alteration or processing of records, photos, or scenes with the intent of defaming, offending, attacking, or invading the privacy of others.

Lost, Stolen, or Damaged Devices*:*

Each user is responsible for their own device and should use it responsibly and appropriately. The schoolwill take no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices.

Responsibilities of the school:

1. Provide a safe network structure and access to Internet that enables the comprehensive use of the laptop.
2. The school will make every effort to ensure that students understand the routines and expectations forthe safety and care of the devices brought to school. Teachers will help children to identify how to keep personal devices secure, but children have the final responsibility for securing their devices.
3. Provide support to access the school's dedicated systems and applications.
4. Provide temporary laptop for students to borrow if their laptop is not working.
5. Provide technical support and advise to fix hardware and software issues which can be resolved withoutdismantling the laptop's parts.
6. Educate students on routines and expectations for the safety and care of their devices
7. The school shall not be liable for any damages or theft occurs on the school's premises.