Shining Star
International School

SHINING STAR INTERNATIONAL SCHOOL
ABU DHABI

BRING YOUR OWN DEVICE POLICY (BYOD)

DEFINITION(S):

To harness student and staff connectivity to personal devices for the purpose of developing 21st century teaching and learning skills BYOD (Bring Your Own Device) is planned. Students bring their personal electronic tabs/laptops as it fosters digital literacy, fluency and social responsibility in a safe environment.

Purpose(s):

The UAE Vision 2021 clearly challenges us to address a "complete transformation of the current education system and teaching methods. The National Agenda aims for all schools, universities and students to be equipped with Smart systems and devices as a basis for all teaching methods, projects and research".

Never has this challenge been more pertinent than in the current times of Covid-19 and our experiences at Shining Star International School of implementing an effective Distance Learning programme of study.

We already use a variety of technology, software and tools to support outstanding opportunities and engagement in learning. However, in order to maximise opportunities for students and teachers to use technology effectively and efficiently, the school will implement a Bring Your Own Device (BYOD) policy which asks students to bring a personally owned device to school to support and enhance learning. Having constant access to a device will allow classrooms to increase learning opportunities and support collaboration through technology.

Rationale:

The use of personal mobile devices at school deepens learning, is personalised and student-centered, and meets the expectations of teachers, students, parents and guardians. At Shining Star International School students and staff are permitted to bring their own personal mobile electronic devices to school for the purpose of learning/teaching. This policy is applies to only those devices recommended by Shining Star International School as being relevant to student learning.

Responsibilities:

At Shining Star International School, we believe that it is of tremendous importance that platforms of knowledge and learning move with the times and be updated on the current technological trends. The school wishes to install good technology habits in children. Bring Your Own Device (BYOD) is a policy where we allow our students to use personal computing devices – such as smart phones, laptops and tablets for educational purposes within the classrooms on our school wireless network.

B.Y.O.D is a technological trend that we believe will have a lasting positive impact on our students' learning. B.Y.O.D will also ensure that more interactive and innovative methods of teaching and learning are introduced using the devices that students have access to both at home and school.

Students:

- Only the internet gateway provided by the school may be accessed while in school. Personal internet connective devices are not permitted to be used to access outside internet sources at any time.
- A student is expected to use his or her device in an ethical manner at all times and adhere to the school's acceptable use policy as outlined in this undertaking.
- Students are prohibited from accessing or storing offensive images, video or audio on Laptops or other digital storage devices.
- Students are prohibited from accessing certain websites during school hours such as Facebook, Twitter and other social networking sites.
- The usage of devices will be recommended by the respective teacher for their classrooms.
- Devices may not be used at any time to store or transmit illicit materials, harass others, download or view/ listen/play music, games, movies and any material which is not related to academics.
- The students are required to place their device in their class device box at the start of every morning. Students are not permitted to keep devices on them or in their lockers.
- The school is not liable for any device stolen or damaged in school; it is the students' sole responsibility to take care of his/her device.
- Protective cases for devices are encouraged.
- Devices must be in silent mode while in school and while riding school buses.
- The student must use the device for educational purposes only and under teacher's supervision.
- The device must not be used to cheat on assignments or tests, or for non-instructional purposes (such as making personal phone calls and text/instant messaging).
- The device must not be used to record, transmit or post photographic images or video of a person, or persons during school hours, unless part of an educational activity under supervision of a teacher.
- The student can only access software on the computer or internet sites which are relevant to the classroom curriculum. Games are not permitted.
- The student must comply with the teachers' request to shut down the computer or close the screen.
- The student must acknowledge that the school's network filters will be applied to their connection to the internet and will not attempt to bypass them.
- The student must understand that infecting the network with a Virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information will result in disciplinary actions.
- The student must realise that processing or accessing information on school property related to "hacking", altering, or bypassing network security policies will result in severe disciplinary actions.
- The school has the right to collect and examine any device that is suspected of causing problems or was the source of an attack or virus infection.

- Student’s device will not have access to school printers and so that printing from personal devices will not be possible at school.
- The device needs to be fully charged prior to bringing it to school and runs off its own battery while at school.

Parents:

- Avoid your child accessing computers in their be droom or rooms that they can “close” off to other members of the family. Encourage use of a central area.
- Set rules for sharing information online and privacy settings of profiles (many universities do online social media checks, so it is important to start right).
- Decide on consequences for misuse of technology and do not hesitate to implement them.
- If you are a technology dinosaur, upgrade yourself!
- Know what social media sites your child is using.
- Also, how your child is using it, what pictures, status updates is your child posting etc.
- Know what games and software your child uses.
- Regularly check their devices for access to inappropriate content.

	Name	Signature	Date
Prepared by:	Dr. Aby Daniel A. Head of Inclusion		20 /09/2024
Policy Review Approved by:	Mrs. Abhilasha Singh (Principal)		03/10/2024

REFERENCES

1. Abu Dhabi Department of Education and Knowledge (ADEK) Guidelines
2. UAE National Cybersecurity Strategy
3. Digital Literacy and Cyber Safety Initiatives in UAE Schools
4. ISTE (International Society for Technology in Education) Standards
5. British Schools in the Middle East (BSME) Technology Guidelines
6. General Data Protection Regulation (GDPR) Compliance for Schools
7. UAE Telecommunications Regulatory Authority (TRA)
8. Common Sense Media BYOD Resources
9. Educational Technology Best Practices by the Knowledge and Human Development Authority (KHDA)

10. UAE Child Protection Law (Wadeema’s Law)