



# Sharjah American International School

## Dubai Campus



# Acceptable Use of Devices Policy

Reviewed on: July 2023

To be Updated on: July 2024

# Contents

<b>Purpose</b> .....	2
<b>BYOD (Bring Your Own Device)</b> .....	2
<b>Acceptable Devices</b> .....	2
<b>General Guidelines</b> .....	3
<b>General Precautions</b> .....	4
<b>Photos, Backgrounds, Music, and Apps</b> .....	5
<b>Lost, Stolen, or Damaged Devices</b> .....	5
<b>Network Connectivity</b> .....	5
<b>Students Responsibility</b> .....	5
<b>Strictly Prohibited Activities</b> .....	6
<b>Social Media</b> .....	6

## **Purpose**

Sharjah American International School – Dubai draws upon most effective, cutting-edge technology in order to enhance teaching and learning practices, improve students’ engagement, and ensure students are college and career ready, especially in today’s digital and technology-oriented world. Utilization of technology in education helps the students become responsible citizens and learn essential 21st century skills such as collaboration, communication, critical thinking, creativity, research, innovation, and problem solving. SAIS Dubai strives to provide appropriate and adequate technology to support instructional purposes. All students in grades 3 to 12 ought to have a device to be able to take advantage of the benefits technology brings into their education. Grades 1 and 2 students are highly encouraged to bring their own devices for the same purpose. An important component of digital learning is being educated about appropriate online behaviors. We review cyber-safety rules with students frequently throughout the course of the school year and offer reminders and reinforcement about safe online behaviors. In addition to the rules outlined in this policy, students are expected to comply with all class and school rules while using school or personal devices.

The use of school technology resources is a privilege, not a right. 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 stated 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 actions shall be applied.

## **BYOD (Bring Your Own Device)**

BYOD are not school devices, but they also fall under the SAIS-D AUP while they are in school premises or are used during school related activities. SAIS-D is not responsible for the repairs, loss, theft, or any damage resulting from their use in school premises or during school related activities.

## **Acceptable Devices**

**Grades 1-8:** Only tablets with iOS operating systems (iPads) are supporting our educational software.

Therefore, iPads (From Apple) are the **ONLY** accepted devices.

- Grades 1 and 2: BYOD
- Grades 3 to 8: Can rent a school device (including the software package and support), or BYOD and get the software package and support from the school.
- All BYOD devices for students in grades 3 to 8 will be added to the school MDM, and the school will have control over these devices until the end of the academic year.

Feature	Minimum Recommended	Preferred
Model	iPad 6 <sup>th</sup> generation	iPad 8 <sup>th</sup> generation iPad Air 5 <sup>th</sup> generation iPad Pro 4 <sup>th</sup> generation
Storage	32 GB	128 GB or above

**Additional recommended accessories:**

- Apple pencil
- Keyboard
- Cover (Back and front)
- Headset with built-in microphone

**Grades 9 to 12 (BYOD Only):**

Feature	Minimum Recommended	Preferred
Processor	Intel Core i5	Intel Core i7 or above
RAM	8 GB	16 GB
Hard Drive	500 GB	1 TB
Operating System	Windows 10 Home	Windows 10 Pro
	Mac OS 10.12	Mac OS 10.15 or higher

**Additional recommended accessories:**

- Touch screens with stylus
- Headset with built-in microphone
- USB memory storage device
- Antivirus

**General Guidelines**

- Students and parents/guardians are expected to adhere to all procedural and safety policies.
- Each teacher has the discretion to allow and regulate the use of the devices in the classroom and on specific projects.
- The device cannot be used unless a teacher has given the permission to use it.
- Approved devices must be in silent mode while on school campus, unless otherwise allowed by a teacher. Headphones may be used with the teacher's permission.
- Devices cannot be used to take unfair advantages during assignments and assessments.

- Devices cannot be used for any non-instructional purposes (such as making personal phone calls and text messaging).
- 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.
- Devices may only be used to access computer files on internet sites which are relevant to the classroom curriculum unless otherwise instructed by the teacher or required by the task.
- Improper use of BYOD will lead to immediate confiscation and permanent 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.
- The school's network filters will be applied to a device's connection to the internet, and any attempt to bypass the network filters is prohibited.
- SAIS-D is authorized to collect and examine any device if it:
  - is suspected of causing technical problems or is the source of an attack or virus infection.
  - infects the network with a virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information.
  - Processes or accesses information on school property related to hacking, altering, or bypassing network security policies.
- Students and parents should be aware that devices are subject to search by school administrators if the device is suspected of a violation of the code of conduct. If the device is locked or password protected, the student will be required to unlock the device at the request of a school administrator.
- Printing from personal devices is not possible at school.
- Personal devices must be charged prior to school and run on battery power while at school. Charging of devices might not be possible at school in all venues.

### **General Precautions**

- School devices are school property, and all users should follow this policy.
- Only use a clean, soft cloth to clean the screen; no cleansers of any type can be used.
- Cords and cables must be inserted carefully into the mobile device to prevent any possible damages.
- School devices (including keyboards) must remain free of any writing, drawing, stickers, or labels.
- School devices left unsupervised are at the users' own risk.
- Devices must always remain in the protective case.

## **Photos, Backgrounds, Music, and Apps**

- The default background photo on school devices and school email account profile photo cannot be changed. These changes will be deemed a violation of this policy.
- Inappropriate material or photos are not to be stored on the school's devices. BYOD devices containing material considered as inappropriate by the school will be confiscated and returned only to a responsible adult. The device may not be brought to school until the offending material/Apps are removed.
- Sound must be muted at all times unless permission is obtained from the teacher.

## **Lost, Stolen, or Damaged Devices**

Each user is responsible for his/her own device and should use it responsibly and appropriately. SAIS-D takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. While school IT Team will help students identify how to keep personal devices secured, students will have the final and full responsibility for securing their personal devices.

## **Network Connectivity**

Users should strive to maintain appropriate bandwidth for school-related work and communications. All users will use the SAIS-D wireless network to access the internet. Students are allowed to connect only to the WiFi assigned to their classes.

Technical malfunctions are always inevitable, and in the rare case that the network is down, the school will not be responsible for lost or missing data.

## **Students Responsibility**

- Students must respect and protect their own and everyone else's privacy by:
  - Using only their assigned accounts.
  - Monitoring all activities on their accounts.
  - Only viewing, using, or copying passwords, data, or networks to which they are authorized to use.
  - Refraining from distributing private information about others or themselves.
  - Turning off and securing the school devices and BYOD devices after they are done using them to protect their work and information.
- Students must respect and protect the integrity, availability, and security of all IT resources by:
  - Reporting security risks or violations to a teacher or supervisor.
  - Not destroying or damaging data, networks, or any other resources.

- Notifying a teacher or supervisor about any device or network malfunctions.
- Students must respect and protect the intellectual property of others by:
  - Following copyright laws (not making illegal copies of music, games, or movies).
  - Citing sources when using others' work (not plagiarizing).
- Students must respect and practice the principles of community by:
  - Communicating only in ways that are kind and respectful.
  - Reporting threatening or discomfoting materials to a teacher or supervisor.
  - Reporting any email containing inappropriate or abusive language or if the subject matter is questionable.

### **Strictly Prohibited Activities**

The following are considered violations and are strictly prohibited:

- Taking pictures or movies of students who have not given their consent to do so.
- Spamming-Sending mass or inappropriate emails
- Transmitting, copying, or creating material that violates the SAIS-D code of conduct.
- Transmitting, copying, or creating material that is illegal.
- Gaining access to other students' accounts, files, or data.
- Using school email for financial or commercial gain or for any illegal activity.
- Bypassing school network filtering through a VPN or web proxy.

### **Social Media**

The internet provides a range of social media tools and apps that allow users to engage and communicate in new, exciting ways. With these new technologies, students have the ability to generate and manipulate content from multiple locations. Users can add images, videos, or links to other media content. Students have unlimited opportunities to individualize the content they embed in their products. The ease of use of these tools encourages student creativity.

It is important to use these technologies and services effectively and flexibly and it is also important to ensure that we balance this with our duties toward our school, the community, our legal responsibilities, and our reputation.

The following guidelines set out a framework of practices that SAIS-D community is expected to follow when using social media:

- Users should not use social media in any way to attack, insult, or abuse school staff, students, their family members, other organizations, or the school.
- In the online environment, users must follow the SAIS-D code of conduct as if they are in school. What is inappropriate in the classroom is inappropriate online.

- Users should not share personal information, including, but not limited to, full name, phone numbers, addresses, birthdates, pictures, security codes, and passwords.
- Users should not discuss personal information about other students, school and the wider community they interact with on any social media.
- Users cannot misrepresent themselves by using someone else's identity.
- Users should know that social media channels are public and information can be shared beyond their control. What you post and share leaves a digital footprint that might have a long-lasting impression on many different audiences.
- When responding to others, users should remember to be respectful and avoid comments that may be hurtful. It is acceptable to disagree with others' opinions; however, do it in a respectful way.
- Comments related to the school should always meet the highest standards of professional discretion.
- Users should not use other people's intellectual property without their permission. It is a violation of copyright law to copy and paste other's thoughts. Pictures may also be protected under copyright laws.
- Users cannot use school email addresses for setting up personal social media accounts or to communicate through such media.
- Use of SAIS-D logos or pictures on your personal social accounts is prohibited. If you wish to promote a specific SAIS-D activity or event, you may do so only by means of a link to the official school accounts.