ARCADIA GLOBAL SCHOOL

AGS BYOD Policy

2024-2026

Al Furjan
Dubai, United Arab Emirates

Purpose:

As part of our endeavor to provide our students with an up-to-date, modern learning experience, Arcadia Global School (AGS) has a BYOD policy for students. We hope that by allowing students to bring their personal devices into school and integrating learning technologies in the classroom, our students will develop research, innovation, and digital literacy skills necessary to be competitive in the modern global workforce. The Bring Your Own Device (BYOD) initiative ensures students learn collaboration, communication, creativity and critical thinking throughout the school day. By allowing students to bring their own device, this will enable students to better access e-learning opportunities while in school, review e-learning tasks directly with their class teachers during in-school days.

Scope:

This policy outlines what the management of AGS expect from students who are using a personal device in their lessons as part of our BYOD initiative. An important component of BYOD will be education about appropriate online behaviours. We will review cyber-safety rules with students frequently throughout the course of the school year and will offer reminders and reinforcement about safe online behaviours. In addition to the rules outlined in these guidelines, students will be expected to comply with all class and school rules while using personal devices. This policy is only applicable to students in Years 3 to 6. Any breach of this policy will result in appropriate investigation and, where necessary, disciplinary action.

Definitions:

Electronic Devices shall include all computing devices that can provide a wireless connection to the Internet. Mobile phones are restricted/not allowed in school. Digital Citizenship is the norms of responsible behavior related to the appropriate use of technology. It encompasses digital literacy, ethics, etiquette, and online safety. User is any individual granted authorization to use electronic devices. Users may include students, parents, staff, volunteers, visitors, contractors, or individuals employed by service providers.

Device Types:

We do not specify a particular brand or model that students must use. But the device specifications of the devices are shared in BYOD FAQ's for Parents reference. They also need to be and safe and convenient to use in school and easy to move around with.

Authorised Use of Electronic Devices:

Electronic devices brought to school shall be restricted to educational and administrative purposes in approved locations and times under the supervision of school personnel.

The school reserves the right to conduct random spot checks on students' devices to ensure that no inappropriate material or Apps are installed.

Authorised users shall:

- Use electronic devices in accordance with the expectations set forth in the school behavior policy.
- Comply with guidelines set by school personnel for the use of electronic devices while on school property or while engaged in a school-sponsored activity.
- Take photographs and audio/video recordings only with a person's consent and when authorised by school personnel for educational purposes.
- Access the school network using approved infrastructure only

Liability

- Students are solely responsible for the care and use of electronic devices they choose to bring to school. Students bringing these devices to school do so at their own risk.
- The school and school personnel shall not be liable for the loss, damage, misuse, or theft of any student-owned electronic device: possessed/used during the school day; in/on school buildings, property, vehicles, or contracted vehicles; during transport to/from school; while attending school-sponsored activities.
- The school and school personnel shall not be responsible for any negative consequences to electronic devices caused by running specific software or by accessing the school network.

Cyber Bullying/Social Media:

Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others. Students will be held accountable for cyberbullying, even if it occurs off-campus during the school year and negatively impacts the academic environment of Arcadia Global School. The Arcadia Global School has zero tolerance for bullying, including cyberbullying, and will take appropriate action against any member of school community who engages in such behaviour in line with our Behaviour Policy.

Responsibilities

1.All Users are Responsible for:

- Registering their electronic device with the school and submitting a signed Use of Electronic Devices Agreement prior to connecting to the school network.
- Ensuring electronic devices are used in accordance with school policies and procedures.
- Caring, maintaining, securing, and storing electronic devices.
- Preserving privacy of accounts, login names, passwords, and/or lock codes to maintain security of electronic devices and data.
- Maintaining safe and productive learning environments when using electronic devices.
- Practicing digital citizenship.

2. All Administrators are Responsible for:

- Informing users of school policy.
- Establishing and monitoring digital citizenship through the School Code of Conduct.
- Responding effectively to disciplinary issues resulting from inappropriate electronic device usage.

- Communicating appropriately with school personnel, parents, and students if school policy is violated from electronic device usage.
- Providing information to users explaining how to connect electronic devices to the school network.

3.Teachers are Responsible for:

- Creating equitable learning opportunities that include electronic devices for education purposes when relevant to curriculum and instruction.
- Determining when students can use school or personal electronic devices for education purposes.
- Supervising student use of electronic devices.
- Responding effectively to disciplinary issues from inappropriate electronic device usage.
- Communicating appropriately with administrators, parents, and students if school policy is violated from electronic device usage.

4.Students are Responsible for:

- Using electronic devices for educational purposes in approved locations under the supervision of school personnel only.
- Implementing virus and malware scanning on their electronic devices.
- Reporting any inappropriate electronic device usage to a teacher or administrator immediately.
- Ensuring their electronic devices are charged prior to bringing them to school.
- Continuing to learn using an alternative method if an electronic device malfunctions.

5. Parents are Responsible for:

- Helping their children take all reasonable steps to care, maintain, secure, store, and transport their electronic device.
- Helping their children preserve the privacy of accounts, login names, passwords, and/or lock codes.
- Identifying the electronic device by labeling it, recording details such as make, model, and serial number, and/or installing tracking software.
- Procuring hazard or theft insurance for an electronic device.
- Encouraging their children to follow school policy and practice digital citizenship.
- Assuming all responsibility for their child's unauthorized use of non-school Internet connections such as a 3G/4G cellular phone network.
- Installing safe search software on child's device.

Guidelines

1. Students must take full responsibility for their own devices. The school is not responsible for the security or transportation of personal devices. Students will take full responsibility for their own devices. Class teachers will advise students on the safe keeping of devices while they are in school.
2. Only the devices that are registered with the school will be allowed for use in the classroom for educational purposes only.
3. Students may only use devices such as tablets, notebooks, small laptops and iPad when in lessons and directed to do so by the supervising teacher. Students are not permitted to use

these devices at lunchtimes, break times or after school whilst still on the premises or at any other times when not directly instructed and supervised by a member of staff.

4. Students must immediately comply with any teacher requests to shut down a device or close the screen. Devices must be in silent mode and put away when asked by teachers.
5. Students are not permitted to capture, transmit or post photographic images/videos of any person on campus for personal reasons or to be posted on public and/or social networking sites.
6. Before recording audio or video or taking a photograph required for an assignment, a student must obtain permission from a teacher who will ensure that all the necessary permissions are taken prior to the event. Recordings and photographs are allowed only for a teacher-approved project or activity.
7. Students should make every effort to charge devices prior to bringing them to school. We have no provision to charge any device in school.
8. To ensure appropriate network filters, students will only use the BYOD wireless connection in school and will not attempt to bypass the network restrictions by using 3G or 4G network or VPNs of any kind. Non-compliance will result in loss of the ability to bring personal devices to school for a period to be determined by the school.
9. Infecting the network with a Virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorised data or information is in violation of the BYOD guidelines and will result in disciplinary actions. The school maintains the right to collect and examine any device that is suspected of causing problems or is the source of an attack or virus infection.
10. Processing or accessing information on school property related to “hacking,” altering, or bypassing network security policies is in violation of the BYOD guidelines and will result in disciplinary actions. Students can only access files on the computer or internet sites which are deemed relevant to the classroom curriculum and suggested by the subject teacher.
11. Printing from personal devices is not available at school.
12. Students must adhere to school rules regarding cyber bullying, digital citizenship and netiquette always.
13. Only One Device (BYOD) per user is allowed to be connected to school Wi-Fi. If a student is changing the device, they should notify the class teacher.
14. School personnel shall not repair or configure user-owned electronic devices.

Netiquette:

- Users should not attempt to open files or follow links from unknown or untrusted origin.
- Recognizing the benefits collaboration brings to education, AGS provides the students with access to web sites or tools that allow communication, collaboration, sharing, and messaging among students. Students are expected to communicate with appropriate, safe, mindful, courteous conduct online and offline.
- Playing commercial/online games and visiting sites not related to education is not permitted. Watching Movies, TV Shows, etc. while at school is prohibited unless the media has been checked out from the school library.
- Respect the use of copyrighted materials. Respect the rights and privacy of others.
- Downloading of unauthorized programs is not allowed.
- Avoid modifying or copying any protected system files, system folders, or control panel files on school equipment.
- Obey the laws and restrictions of UAE, do not use personal equipment to record (audio/visual) of others without their/ school permission and upload them on social media.

- Alert a teacher or other staff member if I see threatening, appropriate, or harmful content (images, messages, posts) online and help maintain the integrity of the school network.
- You should use trusted sources when conducting research via the Internet.

Personal Safety:

- Students should not share personal information, including phone number, address, ID number, passwords or birthday over the internet without adult permission.
- Students should recognize that communicating over the internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others.
- Students should not agree to meet someone they met online in real life without parental permission.
- If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher if you're at school; parent if you're using the device at home) immediately.
- Students should always use the internet, network resources, and online sites in a courteous and respectful manner.
- Students should also recognize that some valuable content online is unverified, incorrect, or inappropriate.
- Students should avoid any irrelevant post online that they would not want parents, teachers, future colleges, employers or the UAE government to see.

Policy Implemented: August 2024
Policy Review Date: August 2026
Policy Responsibility: ICT Lead Engineer
Version: 1