جيمس مودرن أكاديمي
GEMS Modern Academy

B.Y.O.D Policy
2021 – 2022

Approved by:	**Ms.Nargish Khambatta**
Date of review:	**October 2021**
Reviewed on:	**October 2022**
Next Review on:	**October 2023**

Introduction

GEMS Modern Academy (GMA) recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st century technology and communication skills and provide infrastructure access to technologies for student use.

This policy describes the acceptable use of digital technology. It is designed to minimize the risk to students, protect employees and the school from litigation as well as maintain levels of professional standings. The policy is designed to ensure the safe and responsible use of electronic devices by all users, both on the school premises and elsewhere in which the school is represented.

In order to use the school's digital resources, they must follow the guidelines set forth in this this policy. The rules written in this agreement are not all inclusive. GMA reserves the right to change this agreement as when it deems it necessary to do so. It is a general agreement that all facilities (hardware, software, Internet, etc.) are to be used in a responsible, ethical, and legal manner, in and out of school. By using any digital resources, whether owned personally or by the school, users acknowledge their understanding of the BYOD Policy as a condition of using such devices and the Internet. The school provides some electronic devices and services to promote educational excellence. The school has a responsibility to maintain the integrity, operation, and availability of its electronic systems for access and use. The school does not guarantee user privacy or system reliability.

Whilst on site, access to the school network and the Internet should be considered a privilege, not a right, and can be suspended immediately, without notice. Access on site is available only for educational and administrative purposes. Digital resources are to be used in accordance with this Policy and all users will be required to comply with its regulations.

The guidelines provided in this policy are intended to help users understand appropriate use. The school may restrict, suspend, or terminate any user's access to the school's computer systems upon violation of this Policy. This policy applies to all digital resources, not only the computers, devices and equipment provided in the school's IT labs, but also the personal devices students bring to school in accordance with the school's Bring Your Own Device initiative.

The purpose of the 'BYOD Policy' is to ensure that all students use technology in school, at home and elsewhere, effectively, safely and responsibly, to facilitate learning on a 24/7 basis, and to help ensure that they develop the attributes of competent digital citizens.

BYOD Policy provides guidelines for using all digital hardware and software (on individual computers/devices, on local area networks, wide area networks, wireless networks, the Internet and companion technological equipment - e.g., printers, servers, whiteboards, projectors, etc. when students are at school). The Agreement also establishes rights and responsibilities for all users, in and out of school. All users of the school network and technological devices anytime,

anywhere, are expected to follow the guidelines or risk loss of digital privileges. In cases of serious breaches, further action may be taken, in line with the school's standard disciplinary procedures.

School Network Accounts

- Accounts on the systems at GMA are considered secure, although absolute security of any data cannot be guaranteed.
- Students should not store commercial software, music, and/or games or hidden files to their school network account profile folders.
- School-related files are the only files to be saved in a school network account Profile folder temporarily and should be emailed to student personnel email or saved in their fusion virtual learning environment profiles.
- Use only their account/password. This practice will ensure that only their personal device is connected to the network.

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 content.
- Should not to post anything online that they wouldn't want parents, teachers, future colleges, employers or the UAE government to see.

Equipment

- GMA encourages students the use of latest devices as these will ensure compatibility and appropriate educational apps and programmes to be easily installed. The school highly recommends the use of an iPad for Primary / secondary students and Windows Laptop/MacBook laptops for senior students. (More details is added at the end of this document)
- Phones are not used at school at any time, unless explicit permission has been given by the Principal. Students are able to use the phone after school. If students need to contact parents at any time this is allowed via the reception phone
- Only One Device (BYOD) per user is allowed to be connected to school Wi-Fi
- Borrowing of School equipment is not permitted unless email authorization has been given from the respective Faculty Leader or Head of Department, and the hardware is part of an established loan scheme
- Equipment problems should be immediately reported to a teacher supervisor. It is prohibited to move, repair, reconfigure, modify or attach external devices to existing information and network equipment
- All equipment must be properly signed-out/in and documented, and work areas kept neat and clean, free from food and drink.
- Users are expected to treat equipment with extreme care and caution; these are expensive devices that are entrusted to their care. Users should report any damage or loss to their Teacher/ supervisor. If a person checksout or borrows any equipment, they are responsible for replacing it or repairing it if it is lost or damaged. GMA will **not** be financially accountable for any loss or damage.

Violations

Will result in a denial of access and possible further disciplinary action. Notification to parents, Suspension of network, technology, or computer privileges, Detention or suspension from school and school-related activities, Legal action and/or prosecution

- Not respecting the values and ethics of the local host culture.
- Giving access of your password to any other user.
- Any attempts to transmit software designed to compromise the operation or security of the school network in any manner
- Install and use of virtual Private networks within the school network and outside.
- Use school technologies to pursue information on illegal activities.
- Any attempts to circumvent the licensing control or the copying of software from the network
- Students should not download or attempt to download any software on to school equipment
- Use or attempt to use another student's assigned hardware, subscriptions, files, or personal information

- Tampering or experimenting with the school network or equipment, including efforts to bypass the school's Internet filters or proxies
- Use school technologies in a way that could be personally or physically harmful
- Attempt to hack or access sites, servers, or content that isn't intended for my use
- Use school technologies to send spam or chain mail
- Plagiarize content I find online and attempt to find inappropriate images/content
- Post personally-identifying information, about myself or others
- Use language online that would be unacceptable in the classroom and/or at home

Monitoring

- The school will use available its firewall and block software/websites to filter objectionable materials on the Internet in order to help ensure the safety of all students.
- Access to the Internet, including web sites, content, and online tools will be restricted in compliance with UAE regulations and GEMS policies.
- Web browsing may be monitored and web activity records may be retained indefinitely. Email usage, web. Posts, chats, sharing, and messaging may be monitored.

Netiquette

- Users should not attempt to open files or follow links from unknown or untrusted origin
- Recognizing the benefits collaboration brings to education, GMA provides 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 as offline.
- Playing commercial/online games and visiting sites not related to education is not permitted. Watching DVDs, 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.
- Installation of software and applications on students' own devices is permitted insofar as it does not conflict with the security requirements outlined above or the primary purpose of such devices as learning tools. 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 permission and upload them
- 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.

Cyber bullying/Social Media

- Cyber bullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking are all examples of cyber bullying. Students should not send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyber bullying can be a crime. Remember that your activities are monitored and retained.

- Students will be held accountable for Cyber-Bullying, even if it occurs off-campus during the school year and negatively impacts the academic environment at GMA. Students are reminded that in the UAE there are extreme consequences for online defamation of character of person or organization.

- The UAE Student Conduct Disciplinary Bylaw and the Federal Decree-Law no. (5) outline that deliberately creating, transferring and publishing photos and comments on Social Media
- (Instagram and WhatsApp) that undoubtedly shows defamation of individuals or staff members or School Leadership of character, dignity and integrity are breaking the law.

Key provisions relevant to schools' excerpts of Federal Decree-Law no. (5) state:

21	Invasion of privacy, including photographing others, or creating, transferring, disclosing, copying or saving electronic photos (just taking a photo or video of someone without their permission, or saving a photo they have posted, is enough). Defamation. Publishing news, photos, scenes, comments, statements or information, even if true and correct. Amending or processing a record, photo or scene for the purpose of defamation of or offending another person or for attacking or invading his privacy.	Up to 6 months' imprisonment +/ fine of AED 150k – 500k

Students need to be fully aware of their responsibilities that is reinforced at school via the curriculum that covers Common Sense Media. This provides the students with a clear understanding of the above conditions within the UAE and includes comprehensive coverage of issues relating to students' own 'digital footprints' and creating a positive online presence, as well as interaction with others.

Educational Activities

- Educational activities may include researching information, producing documents, participating in surveys, reading e-books and using educational Apps to enhance learning engagements.
- The use of the device is at the sole discretion of the teacher.

Digital Citizenship Awareness

- A focus of this initiative is digital citizenship, which is the responsible use of technology.
- Your child will learn digital skills, ethics, etiquette, and online safety. These are important aspects of participating in today's world.

Safe and Secure

- We are a Common Sense Media accredited school and we are conscious of the dos and don'ts of internet safety. To maintain a safe and secure learning environment, a filtered Internet connection will be provided for students.
- They will not be permitted to use a personal broadband connection such as a 3G/4G phone network. Students will only be able to use their device under the direct supervision of their teacher.
- Any unauthorized use can result in the device being confiscated and privileges being revoked.
- Students will be using the device for not more than 20 to 25 minutes
- in class. As per the school policy, use of devices is not permitted in the buses.

Responsibility

- Students are solely responsible for their device. They must bring it fully charged to school. Similar to other personally owned items, school is not liable for loss, damage, misuse, or theft.
- We therefore suggest that the device is properly labelled and device is configured to use Find my IPad or Find the Android Tracker.

Technical Support

Resources will be provided to help students connect their device to the school network. Your child must be familiar with how to use their device, orientation on the same will be provided in class.

Details of devices for Grades 2-5

WHAT DEVICE DO I BUY	
Option 1 Apple IPad 64 GB 9.7 inches	Option 2 Android tablet 64 GB 9.7 inches
Suggestion: In our experience, I-pad devices have been better to use for young students as compared to other devices.	
DO I NEED TO PURCHASE ANY ACCESSORIES?	
A cover is an absolute **MUST HAVE** as are suitable headsets , All other accessories such as screen protectors and stylus are parent choice.	

Details of devices for Grade 6-12 and IB

WHAT DEVICE DO I BUY	
Option 1 Windows Laptop with Latest OS and memory requirement as per the grade and subjects chose	**Option 2** MacBook Air/Pro
Suggestion: A standard laptop with minimum 6-8 GB RAM and min 250GB hard disc seem to work well for most of the students. If students are opting for Media Studies, they must have a discussion with the media teacher before making a purchase decision.	
NETWORK CONNECTION FOR ALL STUDENTS	
Students can log in only one device using the GEMS e learning username and password provided by school. Please do not change the password given.	

For More information please also refer to

- Student Acceptable Use Policy
- Student Internet Safety Policy
- Safeguarding Policy
- GEMS Parents Cyber Security Guide
- Parent School Contract