

Digital Device Acceptable Use Agreement (DDAUA) / Bring Your Own Device (BYOD) Policy

Vision: Grow - Flourish - Achieve

Mission: Growing Flourishing Achievers through an innovative and sustainable learning environment that fosters academic excellence with holistic development.

Digital Device Acceptable Use Agreement (DDAUA)

- GEMS Founders School Masdar City recognises 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.
- The purpose of this agreement is to establish an environment that is reliable, secure, compliant to regulatory obligations, manageable, and conducive to positive pedagogy at school from the perspective of end-user devices. This agreement 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. The rules written in this agreement are not all inclusive. GFA reserves the right to change this agreement as and when it deems it necessary to do so.
- 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 (Year 2 – 8) Policy.
- Please refer to the complete policy on the school website.
- To use the school's digital resources, they must follow the guidelines set forth in this policy. The rules written in this agreement are not all inclusive. GFA 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 Electronic Devices / Digital Resources / BYOD Agreement 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.

The **DDAUA** 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 GFA 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 personal 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 recognise 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 recognise that some valuable content online is unverified, incorrect, or inappropriate content.
- Students should not post anything online that they wouldn't want parents, teachers, future colleges, employers or the UAE government to see.

Equipment

- GFA encourages students the use of the latest devices as these will ensure compatibility and appropriate educational apps and programmes to be easily installed. The school highly recommends the use of tablet devices including iPad or Android for Primary / Secondary students and Mac or Windows laptops for senior students.
- Phones are not used at school at any time, unless explicit permission has been given by the Principal.
- Students may use their 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.
- Equipment problems should be immediately reported to a teacher / SLT / the IT engineer.
- 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 / Year Lead .
- If a person checks-out or borrows an equipment, they are responsible for replacing it or repairing it if it is lost or damaged. GFA will **not** be financially accountable for any loss or damage.

Violations

- 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.
- Plagiarise 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

Mobile Device Monitoring

The school will use available MDM and block software 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.
- Students are not to have WhatsApp connection with staff but are allowed only through registered email only.
- Recognising the benefits collaboration brings to education, GFA 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
- 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 unauthorised 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 you see threatening, appropriate, or harmful content (images, messages, posts) online and help maintain the integrity of the school network.
- Students 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 behaviours, 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 GFA. Students are reminded that in the UAE there are extreme consequences for online defamation of character of person or organisation.

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).	Up to 6 months' imprisonment +/- fine of AED 150k – 500k
	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.	

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.



Student, School and Parent Agreement

- I acknowledge that I am responsible for my actions on my device, in school, at home and elsewhere, and for following the specific rules established for the use of the hardware, software and networks throughout the school and beyond. I understand that failure to do so could result in a loss of technological privileges.
- I agree that I will not share my passwords or account details with anyone and will have full responsibility for the use of my account. I will not use another's account or represent myself as someone else.
- I agree that I will not engage in illegal activities on the school network or any other digital environment (e.g. plagiarism, bullying, harassment, tampering with hardware, software or documents, vandalism, unauthorised entry or destruction of files or deliberate introduction of computer viruses).
- I agree that I will obey procedural safeguards to maintain the performance of the school's network and digital devices.
- I agree that I will respect the rights of others, use appropriate language, and avoid offensive or inflammatory material. I will bring incidents of offensive or inflammatory material directed to myself or others to the attention of a GEMS Education staff member.
- I agree that I will not share, make, or post online, personally identifying information about any members of the GFA community without permission (addresses, phone numbers, email addresses, photos, videos, etc.).
- I agree that I will access only those resources that are appropriate for school and those resources for which I have specific authorization.
- I agree that I will obey copyright laws and license agreements. Text material, music, software, and other media are protected by law.
- I agree that I will not install software on the school's network or digital devices without permission of the system administrators.
- I agree that I understand that system administrators and teachers may access my files during system maintenance or as a directed action.
- I agree that students who are issued school devices are responsible for their care. Charges related to repair and replacement caused by abuse, misuse, negligence or loss as determined by school administration will be the responsibility of the student and his or her parents.

I acknowledge that my son/daughter and I have read the above and understood its content and I am fully competent to give my consent. And will instruct my child regarding the importance of following guidelines included in this Acceptable Use agreement. I have signed the Summary document that show that I have read and accepted all content included.

Parent/Guardian

Name:

Signed:

Relationship to child:

Date:

Student

Name:.....

Signed:



Monitoring and review

This policy will be reviewed and updated annually or as needed. Within school, the Senior Leadership team will report regularly to the Principal and LAB members concerning the effectiveness of the policy.

Signed Date 01/07/25
Principal/CEO

Next policy review date: 1 July 2026

Appendix A

E-safety Behaviour Ladder – As per Ministerial Resolution No. 581

Example of Behaviour Offences (as per the Ministerial Resolution No. (581) of 2018 Concerning Students' Management)	
First Degree Offences	First Category (minor) Violations
	1.1 Being repeatedly late to the morning parade or failing to participate therein without an acceptable excuse. Absence by more than 3% without an excuse.
	1.2 Failing to attend the classes on time repeatedly without an acceptable excuse. Lack of personal hygiene (hair, nails, clothing)
	2.2 Non-compliance with the school uniform or the school sports uniform without an acceptable excuse.
	2.3 Overgrown hair for boys or bizarre haircuts for boys and girls.
	2.4 Not bringing the books and school kits without an acceptable excuse.
	2.5 Non-compliance with the positive behavior rules inside and outside the classroom, such as: keeping calm and disciplined during the class time and making inappropriate sounds inside or outside the classroom.
	2.6 Sleeping during the class time or formal school activities with no justification (after making sure of the student's health status).
	2.7 Eating during the class times or during the morning parade without a justification or permission (after making sure of the student's health status).
	2.8 Non-compliance with presenting homework and assignments given to him / her in a timely manner.
	2.9 Misuse of the electronic devices such as the tablets etc., during the class, including playing games and using headphones inside the classroom.
	2.10 All of what is similar to these offenses as per the discretion of the Behavior Management Committee.



Second Degree Violations	Second Degree Offences (Medium Risk) Can be issued with internal exclusion for 1-3 days / external suspension if repeated. Repeating the irregularities of the first Level more than 3 times 2.1 Not attending the school without an acceptable excuse at any time, including before and after the holidays and ends of weeks and before exams. 2.2 Getting in or out of the classroom during the class time without permission. 2.3 Not attending the school activities and events without an acceptable excuse. 2.4 Inciting quarrel, threatening or intimidating peers in the school. 2.5 Acting in a manner contradicting with the public morals or the public order at the school and with the values and traditions of the society, such as imitating the opposite sex in terms of clothes, appearance, haircuts and use of makeup. 2.6 Writing on the school furniture or school bus seats. Tampering with the alarm bell or the lift. 2.7 Bringing mobile phones or misuse any means of communication. 2.8 Verbally abusing or insulting students, staff, or visitors of the school. 2.9 Smoking or possessing the relevant kits inside the school campus. 2.10 Refusing to respond to the instruction of inspection or to hand over the banned materials. 2.11 All of what is similar to these offenses as per the discretion of the Behavior Management Committee
Third Degree Offences	Third Category Violations (Serious / Dangerous) Can be issued with bus bans or external suspension. 3.1 Various types and forms of bullying. 3.2 Copying or reproducing the assignments, reports, researches or projects and taking credit for them. 3.3 Getting out of the school without permission or absconding during the school day. 3.4 Attempting to defame peers and the school staff via the social media or abusing them. 3.5 Impersonating others' personality in the school, during transactions, or forging the school documents. 3.6 Destroying or seizing the school furniture, tools, and vandalism. 3.7 Tampering with or destroying the school buses. Causing harm to the driver, supervisor, or the other road users. 3.8 Assaulting others in the school, without causing any injuries to the victim. 3.9 Driving a private car recklessly inside or around the school campus, and not following the security and safety instructions. 3.10 Capturing, possessing, publishing or disseminating photos of the school staff and / or students without their permission. 3.11 All of what is similar to these offenses, as per the discretion of the Behavior Management Committee



Fourth Degree Offences	Fourth Degree Offences (Very Serious) Suspension from school pending investigation.
	4.1 Using the communication means or social media for unlawful or immoral purposes, or in a manner discrediting the educational institution and its staff or others.
	4.2 Possessing or using arms or blade weapons, or their equivalent inside the school.
	4.3 Committing sexual assault inside the school, the bus or during activities.
	4.4 Assaulting others in the school causing injuries to the victim (corporal abuse).
	4.5 Systematic (pre-planned) or covering up theft.
	4.6 Bringing, possessing, presenting, or promoting information or electronic materials that are unauthorized and inconsistent with the values, morals, public order, and public decency.
	4.7 Sexual harassment inside the school, the bus, or during activities.
	4.8 Leaking questions of the exams or engaging therein, in any way.
	4.9 Setting the school campus on fire.
	4.10 Abusing political, religious, or social figures in UAE.
	4.11 Possessing, bringing, promoting, or using narcotics, medical drugs, or the psychotropic substances inside the school or the school bus, or being under the influence of narcotics, non-prescribed medical drugs or the psychotropic substances.
	4.12 Disseminating or promoting ideas or beliefs on extremism, blasphemy or atheism, or the ones harming the political and social regulations of the society.
	4.13 Disdaining the divinely revealed religions or stirring sectarian strife in the school.
	4.14 All of what is similar to these offenses, which are considered as legally punishable offences, as per the discretion of the Behavior Management Committee.