Cambridge International School

Digital Device and Acceptable Use Agreement Policy

NAME OF POLICY	**Digital Device and Acceptable Use Agreement and Policy (DDAUA)**
APPROVED BY	Principal
LAST REVIEW DATE	AUGUST 2024
NEXT REVIEW DATE	AUGUST 2026
RELATED POLICIES	GEMS Mobile Device Management Monitoring System GEMS Student Passwords Procedures

Introduction

GEMS Cambridge International School, Dubai (CIS) 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. We are committed to helping students develop 21st century technology and communication skills and provide infrastructure access to technologies for student use. **All students in Y3-13 are required to bring a learning device (laptop or tablet) to school each day.**

This policy describes the acceptable use of digital technology. It is designed to minimise 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, users must follow the guidelines set forth in this this policy. The rules written in this agreement are not all inclusive. CIS reserves the right to change this agreement as and 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 the 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 (BYOD) initiative.

The purpose of the **Digital Device and Acceptable Use Policy Agreement (DDAUA)** 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 **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 CIS 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 folders
- School-related files are the only files to be saved in a school network account

- Students must use only their own 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 students see a message, comment, image, or anything else online that makes them concerned for their personal safety, they should bring it to the attention of an adult (teacher if they're at school; parent if they'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 can be 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

- **All students in Years 3-13 should bring a learning device (laptop or tablet) to school each day.** We operate a blended learning model where access to a device is needed in most lessons.
- CIS encourages students to use the latest, up-to-date 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 to be 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. **Phones must remain in bags throughout the day.** The only exception is Post-16 students in the Post-16 area.
- Only one device (BYOD) per user is allowed to be connected to school Wi-Fi.
- Borrowing of School equipment is not permitted unless email authorisation 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 / FL / Head of Year. It is prohibited to move, repair, reconfigure, modify or attach external devices to existing information and network equipment
- All borrowed 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 borrowed 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/ FL / Head of Year. If a person checks-out or borrows equipment, they are responsible for replacing it or repairing it if it is lost or damaged. CIS 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

- Installation and use of virtual private networks (VPNs) within the school network and outside
- Using 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
- Students should not 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 that student's use.
- Using school technologies to send spam or chain mail
- Plagiarising content found online and attempting to find inappropriate images/content
- Posting personally-identifying information, about the student or others
- Using language online that would be unacceptable in the classroom and/or at home

Mobile Device Monitoring (MDM)
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 websites, 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 or any other Telephone or social media connection with Staff. Communication is through registered email only
- Recognising the benefits collaboration brings to education, CIS provide 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 they would 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 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
- 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 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 CIS. 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) outlines that deliberately creating, transferring and publishing photos and comments on Social Media (Instagram, WhatsApp, Snap Chat, TikTok, Discord, etc) 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 are reinforced at school via the curriculum that is delivered using materials from 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.

Digital Device Acceptable Use Agreement (DDAUA)

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. CIS reserves the right to change this agreement as and when it deems it necessary to do so. Please refer to the complete policy on the school website.

The Agreement Essentials:
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 CIS 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 authorisation.

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/her parents.

I acknowledge that my son/daughter and I have read the CIS Digital Device Acceptable Use Agreement (DDAUA) that is on the CIS website and will instruct my child regarding the importance of following all the guidelines included in this agreement.

Parent Signature _____ Date_____