مدرسة جيمس كامبردج العالمية أبوظبي
GEMS Cambridge International School
ABU DHABI

ICT Acceptable Use Policy for Learners

Reviewed by	David Craggs
Date of review	September 2021

ICT Acceptable Use Policy for Learners

Rationale

The use of the latest technology is actively encouraged at GEMS Cambridge International School – Abu Dhabi, but with this comes a responsibility to protect learners, staff and the School from abuse of the system.

All learners, therefore, must adhere to the policy set out below. This policy covers all workstations, laptops, mobile telephones and other electronic devices within the school, irrespective of who the owner is.

All learners are expected to behave responsibly on the school computer network, as they would in classrooms and in other areas of the School.

Aims

The purpose of the GEMS Cambridge International School – Abu Dhabi's ICT Acceptable Use Policy is to ensure that all learners 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 ICT Acceptable Use Policy provides guidelines for using 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 learners 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 standard behaviour policy.

The signatures on the Letter of Agreement (located at the end of this document) are binding and indicate that the parties who signed have read the terms and conditions and understand their meaning.

Users who knowingly access prohibited information or who disregard guidelines will be subject to disciplinary action.

1. *Personal Safety*

- Always be extremely cautious about revealing personal details and never reveal a home address, telephone number or email address to strangers.
- Always inform your teacher or another adult if you have received a message or have visited a website that contains inappropriate language or makes you feel uncomfortable in any way.
- Do not play with or remove any cables that are attached to a School computer.
- Always be yourself and do not pretend to be anyone or anything that you are not on the Internet.
- Do not arrange to meet anyone you have met on the Internet; people are not always who they say they are.
- If in doubt, ask a teacher or another member of staff.

2. *System Security*

- Do not attempt to go beyond your authorised access. This includes attempting to log on as another person, sending e-mails whilst masquerading as another person or accessing another person's files. Attempting to log on as staff is unacceptable and may result in the loss of access to systems and other serious sanctions. You are only permitted to log on as yourself.
- Do not give out your password to any other learner; if you do and they do something wrong logged on as you, you will be held responsible. If you suspect someone else knows your password, change it immediately.
- Do not alter School hardware in any way.
- Do not eat or drink whilst using the computer.

3. Inappropriate Behaviour

'Inappropriate Behaviour' relates to any electronic communication whether email, blogging, tweeting, social networking, texting, journal entries or any other type of posting/uploading to the Internet.

- Do not use indecent, obscene, offensive or threatening language.
- Do not post or send information that could cause damage or disruption.
- Do not engage in personal, prejudicial or discriminatory attacks.
- Do not harass another person. 'Harassment' is persistently acting in a manner that distresses or annoys another person
- Do not knowingly or recklessly send or post false, defamatory or malicious information about a person
- Do not post or send private information about another person without their prior agreement.
- Cyber-Bullying of another person either by email, online or via texts will be treated with the highest severity. Learners will be held accountable for Cyber-Bullying, even if it occurs off-campus during the school year and negatively impacts the academic environment at GEMS Cambridge International School – Abu Dhabi.
- Parents and learners in all grade levels using any social media forums must, at all times, demonstrate respect for the members of the school community (including all learners and personnel)
- Parents and learners must not breach confidentiality, defame or make threats to any person in the school community; including but not exclusive to the use of WhatsApp, Snapchat, Messenger and Instagram
- Do not access, or post, material that is profane or obscene, or that encourages illegal acts, violence or discrimination towards other people.
- If you mistakenly access such material, please inform your teacher or another member of staff immediately or you may be held responsible.
- Do not attempt to use proxy sites on the Internet.
- Do not take or post a photo of another learner or member of staff without their permission.

4. Email & messages

- You should check your personal email and MS Team messages at least once a day during term time for new messages.
- Do not reply to spam mails as this will result in more spam. Delete them and inform the IT support office.
- Do not open an attachment from an unknown source. Inform the IT support office as it might contain a virus.
- Do not use email (including web mail) during lessons unless your teacher has given permission.
- Do not send or forward annoying or unnecessary messages to a large number of people, e.g. spam or chainmail.

5. Plagiarism and Copyright

- Plagiarism is taking the ideas or writings of others and presenting them as your own. Do not plagiarise works that you find on the Internet or anywhere else.
- You should respect copyright. Breaking copyright law occurs when you reproduce a piece of work. You should request permission from the copyright owner. This includes music files and the copying of CDs, downloading of films from illegal sites and other such formats.

6. Privacy

- All files and emails on the system are the property of the School. As such, system administrators and staff have the right to access them if required.
- Do not assume that any email sent on the Internet is secure.
- All network access, web browsing and mails on the School system are logged.
- If you are suspected of breaking this Policy, your own personal laptop/device and mobile telephone can be searched by staff.
- The School reserves the right to randomly search the Internet for inappropriate material posted by learners and to act upon it.

7. Software/hardware

- Do not install any software on the School system.
- Do not attempt to download programmes from the Internet onto School computers.
- Do not knowingly install spyware or any sort of hacking software or device.
- Report equipment problems immediately to a teacher or the IT Department.
- Leave workstations and peripherals in their designated places.
- Keep work areas neat and clean and free from food and drink.
- Any attempts to move, repair, reconfigure, modify or attach external devices to existing information and network systems without the Network administration and/or IT Department's permission is prohibited.
- Borrowing of School hardware is not permitted unless email authorisation has been given from the IT department, or the hardware is part of an established loan scheme.

8. Sanctions

- Sanctions will vary depending on the severity of the offence; they will range from a warning or withdrawal of Internet use, to suspension or expulsion.
- A breach of the law may lead to the involvement of the police.

9. General and Best Practice

- Think before you print; printing consumes resources which is bad for the environment.
- Priority must be given to learners wishing to use the computers for School use.
- Always log off your computer when you have finished using it. Do not lock the computer so that others cannot use it.
- Always back up your work if you are not saving it on the School system. Work saved on the School system is backed up every night for you, but be careful if you only have a copy of your work on a memory stick.
- Avoid saving or printing sizeable files (e.g. above 5mb); if in doubt ask a member of IT support.
- Observe Health and Safety Guidelines; look away from the screen every 10 minutes to rest your eyes and make sure your chair is positioned and adjusted to the correct height to the desk.
- Housekeep your email regularly by deleting old mail.
- If a web page is blocked that you feel you have a legitimate use for, please ask IT support and it can instantly be unblocked if approval is given.
- If in doubt, ask a member of the IT support office.

10. *Mobile Phones / Mobile Devices*

- Do not use a mobile telephone or other mobile device during lessons unless you have the teacher's permission.
- Mobile telephones should be switched off and kept out of sight while you are on the school premises unless you have the permission of a teacher.
- Do not take photos or videos with any device during lessons unless the member of staff has given permission.
- Do not take photos of people without their permission.
- Bullying by text or any other method will be treated in the same severe manner as any other form of bullying.
- Do not attempt to hack into someone else's device via Bluetooth or any other method.
- If a learner needs to use a phone in an emergency then they are able to go to their Head of Year (in the first instance), the reception or their Head of School office.
- If a learner is found to be using a mobile phone without permission, then they are to be warned for 'Inappropriate use of device' in the first instance.
- If a learner repeatedly uses their phone then the curriculum leader/Head of Year is to be informed and the teacher is within their right to confiscate the phone from the learner, which can then be collected at the end of the school day.
- Teacher's must store any confiscated phones in a secure location and be available at the end of the day to return it to the learner in an agreed location.
- Learners are allowed to use their phones at the end of the school day, once they reach the ground floor.

11. *Music/Video Players (e.g., iPods, Earpods)*

- The use of such devices is banned during lessons.
- Do not connect such a device to the School network/School computers.
- Learners should not be wearing earpods on the school premises.
- Do not break copyright laws by swapping illegal music/video files.

12. *Personal Equipment*

- Watching DVD's, Movies, TV Shows, etc. while at school is prohibited unless the media has been checked-out from the school library or has been provided by The School's streaming server.
- Private networks are prohibited within the school network unless users get permission from the IT Department.
- The safety and security of your personal devices including but not limited to; Laptops, Tablets and Mobile telephones is your responsibility whilst at school.
- The Primary device that you connect to the school Wi-Fi network should always be fully charged before bringing it to school.

I have read and understood and agree to comply with the Learner ICT Acceptable Use Policy.

Signed (learner): …… Print Name: …… Date: ……

Section (Form Class): ……....

Student ID (OASIS Number): ……....

Signed (parent): …… Print Name: …….. Date: ……