MANAGING MOBILE TECHNOLOGIES

PURPOSE

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to access data from a mobile device connected to CPS Network. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet computers.
- Ultra-mobile PCs (UMPC).
- Tablets
- Wearables and other mobile devices

TAKING CARE OF SCHOOL MOBILE DEVICES

CPS may provide users (staff and students) with mobile devices to promote learning both inside and outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to IT Administrator immediately. Users may be financially accountable for any damage resulting from negligence or misuse. School mobile devices that are broken or fail to work properly at the time they are in the custody of the students or staff must be taken promptly to the Staff/IT technician for an evaluation of the equipment.

General Precautions

- School mobile devices are school property and all users will follow this policy and the acceptable use policy for technology.
- Only use a clean, soft cloth to clean the screen, no cleansers of any type.
- Cords and cables must be inserted carefully into the mobile device to prevent damage.
- School mobile devices must remain free of any writing, drawing, stickers, or labels.
- School mobile devices left unsupervised are at the user's own risk.
- For personal devices, parents must ensure their child's mobile device comes to school fully charged and loaded with Apps requested by the school.
- Students below grade 3 should never to take the Mobile devices outside the classroom without supervision or approval
- Do not leave the mobile device in an open carry bag so as to prevent it from falling out or from theft.

Carrying Mobile devices

Users are requested to use a protective cover for mobile devices with sufficient padding to protect it .The guidelines below should be followed:

- School mobile devices must always remain within the protective case when carried.
- Only one mobile device should be carried at any one time.

Screen Care

The mobile device screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen.

- Do not lean on the top of the mobile device when it is closed.
- Do not place anything near the mobile device that could put pressure on the screen.
- Do not place anything in the carrying case that will press against the cover.
- Clean the screen with a soft, dry cloth or anti-static cloth.
- Do not “bump” the mobile device against lockers, walls, car doors, floors, etc as it will eventually break the screen

Using Mobile and BYOD devices at School

Mobile devices and BYOD devices are intended for use at school each day. In addition to teacher expectations for Mobile device and BYOD use, school messages, announcements, calendars and schedules may be accessed using the mobile device and BYOD. The mobile device or BYOD cannot be used unless a teacher has given permission for its use.

.

Sound, Music, Games, or Programs

- Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.
- Music and Internet Games on the school mobile devices may be allowed at the discretion of the teacher.Installation of 3rd party applications on school mobile devices should be done by authorized school staff only.
- All Apps on BYOD are the financial responsibility of the student’s family. The required Apps mustbe installed and updated at home.

MOBILE DEVICE MANAGEMENT

CPS will use Mobile device management/ End point protection software to monitor and manage the safe use of mobile devices within the campus. The students/ Staff must have to use the device in the campus as per the instructions from the Teacher’s / Line manager. Users shall not try to bypass the security policy applied on the device by any means. Violating this policy will result in disciplinary actions

Inspection

Students may be selected at random regularly to provide their device for inspection including BYOD to ensure that there are not any violations to this policy.

MANAGING MOBILE TECHNOLOGIES

ACCEPTABLE USE

This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the User Terms and Conditions named in this policy, privileges will be terminated, access to the school's technology resources will be denied, BYOD devices will be denied access to the school's network and Wi-Fi facilities and the appropriate disciplinary action shall be applied.

Parent/Guardian Responsibilities

Parents have a responsibility to talk to their children about values and the standards that their children should follow regarding the use of the Internet as they would in relation to the use of all media information sources such as television, telephones, movies, radio and social media.

Parents may opt out of allowing their child to use the school mobile devices or BYOD. To opt out parents must sign a form indicating this and acknowledging that their child is still responsible for meeting the learning expectations.

School Responsibilities are to:

- Provide Internet access to its students.
- Provide firewall filtering to block access of inappropriate materials where possible.
- Provide data storage space. These will be treated similar to school lockers. the school reserves the right to review, monitor, and restrict information stored on or transmitted via school owned equipment and BYOD devices and to investigate inappropriate use of resources.
- Provide staff guidance to aid students in doing research and help assure student compliance of the acceptable use policy.

Students are Responsible for:

- Using computers/mobile devices in a responsible and ethical manner.
- Obeying general school rules concerning behavior and communication that apply to CPS online safety policy
- Using all technology resources in an appropriate manner so as to not damage school equipment. This "damage" includes, but is not limited to, the student's own negligence, errors or omissions.
- Helping the school protect our computer system/device by contacting an administrator about any security problems they may encounter.
- Students should always turn off and secure the mobile device and BYOD devices after they are done working to protect their work and information.
- If a student receives any message on an online platform containing inappropriate or abusive language or if the subject matter is questionable, he/she is asked to report the matter to the teacher
- Ensuring all BYOD devices are fully charged at the start of the school day.
- Their BYOD device is brought to school each day unless otherwise informed.

- Ensure their BYOD device has the Apps/software installed as requested by the school and maintain software upgrades.

Student Activities Strictly Prohibited:

- Illegal installation or transmission of copyrighted materials
- Students must not take pictures or videos of any other student.
- Any action that violates existing school policy or public law
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, religious or sexually explicit materials
- Use of chat rooms, online games and other forms of social media communication
- Internet/Computer Games without permission of the school.
- Changing of school mobile device settings (exceptions include personal settings such as font size, brightness, etc)
- Downloading apps at school unless supervised by the teacher and parental consent.
- Spamming-Sending mass or inappropriate emails
- Gaining access to other student's accounts, files, and/or data
- Use of the school's internet/E-mail accounts for financial or commercial gain or for any illegal activity
- Use of anonymous and/or false communication applications
- Students are not allowed to give out personal information, for any reason, over the Internet. This includes, but is not limited to, setting up internet accounts including those necessary for chat rooms.
- Participation in credit card fraud, electronic forgery or other forms of illegal behavior.
- Vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of school equipment will not be allowed
- Bypassing the school web filter through a web proxy.

Mobile device and BYOD Care

- Students will be held responsible for maintaining their own devices and keeping them in good working order whilst in their possession.
- BYOD devices must be recharged and ready for school each day.
- The school will be responsible for repairing only school owned Mobile devices that malfunction. Mobile devices that have been damaged from student/staff misuse or neglect will be repaired with cost being borne by the student/staff. In the event of an accidental damage, the school on a case-to-case basis may exercise discretion in recovering the cost of repair to the device from the user.

Mobile device theft

- Mobile devices that are stolen must be reported immediately to IT Helpdesk/Principal and may require further reporting to the local Police.

Legal Propriety

- Comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity.
- Plagiarism is a violation of the School code of conduct / behavior policy. Give credit to all sources used, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text.
- Use or possession of hacking software is strictly prohibited and violators will be subject to consequence. Violation of applicable law will result in criminal prosecution or disciplinary action by the school.

Protecting & storing of the Mobile and BYOD devices

Mobile devices and BYOD will be labelled in the manner specified by the school. Students / Staff are not allowed to change/ tamper the identification stickers/ serial number info on any devices.

AUP/BYOD User Pledge

1. I will only use the School facilities, equipment and Internet when these are officially available for my use.
2. I will only access my account and make sure no one else has access to my account. I understand that I am responsible for all actions that take place on my user account.
3. I will not download, transfer, write, draw or view any unsuitable graphic, text or other inappropriate material and it is my responsibility to immediately inform the teacher should I accidentally access anything inappropriate.
4. I will not download, transfer, install or use any applications, utilities, games, music, video files or other files or software not approved by the School.
5. I will only access websites as directed by my teacher.
6. YouTube, gaming sites, and social networking sites are expressly forbidden unless authorised.
7. I will not partake in any type of cyberbullying and I will report any cyberbullying to a staff member.
8. I will treat the School computers, systems and the school network with respect and care.
9. If I know of someone misusing anything, I will report this to a member of staff anonymously.
10. I will only access the local server or wider network that is readily available to me.
11. If I use any material from the Internet in my own work, I will clearly state the source.
12. I will only use e-mail, chat or messaging facilities during lessons if allowed.
13. I will only use the schools network for transmission and reception of material that would be considered acceptable by the school
14. I will only use my school e-mail address responsibly and appropriately at all times.
15. I will not eat or drink whilst using the ICT facilities and equipment.
16. I will not interfere with the work of others.
17. I will not attempt by any means to bypass the restrictions placed upon the machine or the network I am connected to.
18. I understand that I should not attempt to bypass the blocking put in place by the law of the UAE
19. I will never attempt to “jailbreak” the school Mobile device or attempt any repairs.
20. I will not place decorations (such as stickers, markers, etc.) on the school Mobile devices. I will not deface the serial number Mobile device sticker on any Mobile device.
21. I understand the school Mobile device remains the property of the School.

The following applies for BYOD devices

22. I will take good care of my BYOD device.
23. Students will not use devices on school transport, in public areas of the school, during the school day, unless permitted.
24. I will only use my device for educational purposes as and when requested.
25. I will never leave the BYOD device unattended.
26. I will never loan out my BYOD device to other individuals.
27. I will keep food and beverages away from the BYOD device since they may cause damage to the device.
28. I will use the BYOD device in ways that are appropriate, meeting School expectations.
29. Students understand that the BYOD device is subject to inspection at any time without notice.
30. I will ensure that anti-virus and anti-malware software is installed on my BYOD and is kept updated regularly and frequently.
31. I understand that my personal device is my responsibility and School is not responsible for any breakages, lost, theft or any damage caused by malware on the network
32. I will follow the policies outlined in the CPS Acceptable Use Policy

Prepared By	Reviewed/ Checked	Approved By
IT Administrator (IT Support Coordinator)	Vice Principal (Online safety Coordinator)	Principal (Online Safety Leader)

.