E-SAFETY AND BRING YOUR OWN DEVICE (BYOD) POLICY		
Applicable to	☒Schools ☐Nurseries	
Teams / Individuals	☒Academic Staff ☒Administration Staff	
Publishing Channel	☒Parents' VLE ☒Staff Dashboard ☒Website ☐Dept. Micro-site	
Linked Policies	Behaviour for Learning Policy Safeguarding & Child Protection Policy Positive Relationship Policy Counselling Policy Health & Safety Policy Positive Relationships Policy Positive Education and Emotional Wellbeing Policy Information & Data Protection Policy	
Linked Documents	Code of Conduct for Students	
Updated By	**Latest Publish Date**	**Monitoring Cycle**
Dr Neil Hopkin	August 25	Annual
Version No.	**Amendments**	
1.0	None	
1.1	Liability Clause added	
1.2	Logo	
1.3	Mobile phones on campus clarification	
1.4	Formatting	

POLICY BRIEF AND RATIONALE

The focus of Sunmarke school is to provide tools and resources to the 21st Century Learner. Excellence in education requires that technology is seamlessly integrated throughout the educational program. Increasing access to technology is essential for that future. This empowers the students to maximize their full potential and to prepare them for college and the workplace.

Learning results will improve from the continuous dynamic interaction among students, educators, parents, and the extended community. Technology immersion does not diminish the vital role of the teacher. To the contrary, it transforms the teacher from a director of learning to a facilitator of learning. Effective teaching and learning with wireless technology tools integrate technology into the curriculum anytime, anyplace.

BYOD, while not school property, also falls under this policy whilst on school property or whilst on school related activities.

The policies, procedures and information within this document apply to all wireless mobile devices used at Fortes Group of Schools, including any other device considered by the Administration to come under this policy. Teachers may set additional requirements for use in their classroom.

Parents MUST understand and acknowledge that the **school does not assume any responsibility for lost or misplaced or damaged devices, and it is the students' sole responsibility to ensure the safekeeping of their personal electronic devices at all times.**

Parents hereby waive, release, and discharge the School and the School's owners, shareholders, investors, staff, agents, contractors, employees, servants, consultants, and invitees from any and all loss, damage, claims, demands, actions, costs, expenses and liabilities of whatsoever nature arising out of any loss or damage of their child's personal electronic device.

USER BEHAVIOUR

Using BYOD/school devices at School

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

a. Screensavers / Background photos / Apps

The screensaver or background photo may not be changed for any reason on any school mobile devices. Any changes to the display of the school mobile device will be deemed a violation of this policy.

Passwords are not to be used on school mobile devices.

Inappropriate material or photos are not to be stored on school devices or BYOD. BYOD containing material considered inappropriate by the school will be confiscated and returned only to a responsible adult. The device may not be brought to school until the offending material/Apps are removed.

b. Sound, Music, Games, or Programs

- Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.
- Music is allowed on the mobile device and can be used at the discretion of the teacher.
- Internet Games are not allowed on the school mobile devices. If game apps are installed on school mobile devices, it will be by Fortes staff only.
- All software/Apps must be school provided (school mobile devices only).
- All Apps on BYOD are the financial responsibility of the student's family. School required

Apps must be reloaded at home.

c. Saving to the Mobile device/Home Directory

Students may save work to the home directory on the mobile device - but it will not be backed up in case of re- imaging. It is recommended that data storage be via One Drive provided by the school and accessed via the student's office 365 account. The accounts set up will be completed by Fortes Staff. Please note that the school reserves the right to access these accounts. BYOD owners must not store personal information on the school acquired third party storage area to avoid any privacy issue violation.

It is the student's responsibility to ensure that work is not lost due to mechanical failure or accidental deletion. Mobile device malfunctions are not an acceptable excuse for not submitting work.

d. Inspection

Students may be selected at random to provide their device for inspection including BYOD to ensure that there are no violations to this policy.

e. Procedure for re-loading software

If technical difficulties occur and illegal software or non-Fortes installed apps are discovered, the school mobile device will be restored from backup. The school does not accept responsibility for the loss of any software or documents deleted due to a re-format and re-image.

f. Software upgrades

Upgraded versions of licensed software/apps are available from time to time. Mobile devices may be removed from circulation for periodic updates and synching. All BYOD devices are expected to update software at home and not during the school day.

g. Social Media

- Be aware of what you post online. Social media venues including wikis, blogs, photo, and video sharing sites are public. What you contribute leaves a digital footprint for all to see. **Do not post anything you wouldn't want friends, parents, teachers, or a future employer to see. It is your responsibility to ensure that your use of social media conforms with the laws of the UAE.** Students should be especially aware of the laws surrounding defamation, video recording, and video sharing.
- Follow the school's code of conduct when writing online. It is acceptable to disagree with someone else's opinions, however, do it in a respectful way. Make sure that

criticism is constructive and not hurtful. What is inappropriate in the classroom is inappropriate online. Once again, students are reminded about the strict laws about defamation in the UAE.

- Be safe online. Never give out personal information, including, but not limited to, last names, phone numbers, addresses, exact birthdates, and pictures. Do not share your password with anyone besides your teachers and parents.
- Linking to other websites to support your thoughts and ideas is recommended. However, be sure to read the entire article prior to linking to ensure that all information is appropriate for a school setting.
- Do not use other people's intellectual property without their permission. It is a violation of copyright law to copy and paste other's thoughts. When paraphrasing another's idea(s) be sure to cite your source with the URL. It is good practice to hyperlink to your sources.
- Be aware that pictures may also be protected under copyright laws. Verify you have permission to use the image.
- How you represent yourself online is an extension of your personal image. Do not misrepresent yourself by using someone else's identity.
- Blog and wiki posts should be well written. Follow writing conventions including proper grammar, capitalization, and punctuation. If you edit someone else's work, be sure it is in the spirit of improving the writing.
- If you run across inappropriate material that makes you feel uncomfortable, or is not respectful, tell your teacher right away.
- Students who do not abide by these terms and conditions may lose their opportunity to take part in projects and/or access to future use of online tools.

SCHOOL RESPONSIBILITIES

- Provide Internet and Email access to its students.
- Provide Internet Blocking of inappropriate materials where possible.
- Provide data storage areas. These will be treated like school lockers. Fortes reserves the right to review, monitor, and restrict information stored on or transmitted via Fortes 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' full names will not be used anywhere on the website, particularly in association with photographs.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of

internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

E Safety Complaints Handling

- Complaints of internet misuse involving the students are through CPOMS. Sanctions resulting may include interview / counselling by the Teacher / Principal, informing parents or carers, removal of internet or computer access for a period of time.
- Complaints of a child protection nature must be dealt with in accordance with the school's Safeguarding & Child Protection Policy.

STUDENT RESPONSIBILITIES

- Using computers/mobile devices in a responsible and ethical manner.
- Obeying general school rules concerning behavior and communication that apply to Technology equipment use.
- Using all technology resources in an appropriate manner so as to not damage school equipment. This "damage" includes, but is not limited to, the loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by the student's own negligence, errors, or omissions.
- Use of any information obtained via Fortes designated Internet System is at your own risk. Fortes specifically denies any responsibility for the accuracy or quality of information obtained through its services.
- Monitoring all activity on their account(s).
- 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 should receive an email containing inappropriate or abusive language or if the subject matter is questionable, he/she is asked to print a copy and turn it in to the Head of School's office.
- Returning the school mobile device to the class teachers at the end of each period/s or day.
- 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.

- Students will be held responsible for maintaining the individual Mobile devices and keeping them in good working order whilst in their possession.
    - If a student has borrowed the Mobile device from school and it is found unsupervised, the student may have their borrowing privileges revoked for the remainder of the academic year.
    - Mobile devices that malfunction or are damaged must be reported to the IT Technician. The school will be responsible for repairing only school owned Mobile devices that malfunction. Borrowed mobile devices that have been damaged from student misuse, neglect or are accidentally damaged will be repaired with cost being borne by the student. Students will be responsible for the entire cost of repairs to Mobile devices that are damaged intentionally.
- Mobile device damage: Students are responsible for all damage.
- Mobile devices that are stolen must be reported immediately to the Office and the Police Department.

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.

STUDENT ACTIVITIES STRICTLY PROHIBITED

- Illegal installation or transmission of copyrighted materials.
- 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, sites selling term papers, book reports and other forms of student work.
- Internet/Computer Games.
- Use of outside data disks or external attachments without prior approval from the administration.
- 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.

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 Fortes Behaviour for Learning 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 dealt with by appropriate disciplinary action. Violation of applicable law will result in criminal prosecution or disciplinary action by the school.

CYBER-BULLYING

Cyber-bullying is an aggressive, intentional act carried out by a group or an individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself.

By cyber-bullying, we mean bullying by electronic media:

- Bullying by texts or messages or calls on mobile phones
- The use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, or humiliating material on websites, blogs, personal websites, social networking sites
- Using e-mail to send threatening messages to others
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, defamatory, or humiliating remarks in chat rooms, Facebook, YouTube etc.

School Actions against Cyber-bullying

- The school supports victims and, when necessary, will work with the Police to detect those involved in criminal acts.
- The school will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, both in and out of school.
- The school will use its power of confiscation where necessary to prevent pupils from committing crimes or misusing equipment.
- All members of the school community are aware of the fact that they have a duty to bring to the attention of the Principal any example of cyber-bullying or harassment that they know about or suspect.

ACCEPTABLE USE

The use of Fortes technology resources is a privilege, not a right. The privilege of using the technology resources provided by the Fortes Group of Schools is not transferable or extendable by students to people or groups outside the school.

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.

The Fortes Group of Schools Behaviour for Learning Policy and Procedures shall be applied to student infractions.

Violations may result in disciplinary action up to and including suspension/ expulsion for students. When applicable, law enforcement agencies may be involved after KHDA consultation.