Written by:	E-Safety Coordinator/Online Safety Officer	**Reviewed:**	November, 2021
Approved by:	Principal, EAS	**Next Review:**	November, 2022

ACCEPTABLE ICT USE POLICY

Aim

Our aim is to make our school community aware of the possible risks that may occur while using technology and how they can be safe online. Students and staff should be free of fear of cyber bullying anyone known or unknown and should be able to recognize cyber bullying. They should be able to deal with it effectively and ultimately become responsible citizens.

Scope

This policy includes:

- Acceptable use of internet by students
- Acceptable use of internet by staff
- School security systems
- Prohibited use for all users

This policy is aligned with:

- Safeguarding policy
- Anti-bullying policy
- Child protection policy

1. **Acceptable use of school's internet and technology systems for students – School Devices:**

1.1 School devices are the sole property of the school and all users will follow this policy
1.2 School devices are intended for educational use only
1.3 Any school device can be used only after the respective teacher has permitted use
1.4 Music and internet games on school devices are allowed at the discretion of the teacher

1.5 Games. Apps, software, screen saver, backgrounds etc. should not be downloaded on school devices without permission from school ICT department
1.6 Do not change any device settings without permission from ICT department
1.7 Turn off all devices after you are done working on it
1.8 All devices should be used in a responsible manner
1.9 Do not write or label on school devices
1.10 Any damage to the school devices will lead to disciplinary action by school administration

Internet and Technology:

1.11 School internet must be used for educational research and information gathering purpose only
1.12 Attempt online tests and tasks as approved or advised by teachers
1.13 Share emails only with known people or with only those who are approved by parents/teachers
1.14 Maintain confidentiality of personal name, username, password, contact information, files, data etc.
1.15 Do not try to access and change other person's password, files or data
1.16 Do not download prohibited software or content
1.17 Do not view prohibited online content. Report it immediately to your section supervisor if you come across anyone doing so.
1.18 Support the school to protect school systems by contacting teacher/supervisor for any security problems that they may encounter
1.19 Do not share copyrighted materials
1.20 YouTube, gaming sites and social networking sites are forbidden to use
1.21 Do not send, upload, download, or distribute offensive, threatening, obscene or religious materials
1.22 Do not share school copyrighted material (school logo, worksheets, question papers, soft copies of any school owned material)
1.23 Approach your teacher/supervisor and report any activity which seems unusual or confusing to you or if you are facing any form of bullying
1.24 Obey general school rules concerning behaviour and communication

2. **Acceptable use of school's internet and technology systems for staff –**
School Devices:

2.1 School devices are intended for educational use and not for personal matters

2.2 Do not change any device settings without permission from ICT department
2.3 Do not share your username and password with anyone and ensure that you change it at regular intervals
2.4 Do not use the system if the previous user has not logged out. Either log out and use your credentials, or approach the ICT department for support
2.5 Do not save personal files or data on school systems
2.6 Do not download or install any program, software or hardware without permission
2.7 Turn off the devices once you are done working on it

Internet and Technology:

2.8 School network must for used for school matters only and not for personal interest
2.9 All staff members are accountable to report any unauthorized use of the school system or network
2.10 Social networking sites are forbidden to use
2.11 Use the email id provided by school to communicate about school related matters with students/parents/outside community
2.12 Ensure no one has access to your school account
2.13 Do not send, upload, download, or distribute offensive, threatening, obscene or religious materials
2.14 Do not save your personal username, passwords, bank details, contact information etc. over school network.
2.15 Respect materials that have copyrights and think wisely before downloading or forwarding any such data
2.16 Advise and spread awareness among students and colleagues on how to be safe online
2.17 Share best practices involving ICT skills
2.18 Do not share school internet credentials with any visitor/outsider
2.19 Be responsible and ethical while communicating online
2.20 Do not use school's internet or email for financial or commercial gain
2.21 If you notice any unusual activity that seems suspicious, then report to the e-safety coordinator immediately
2.22 Impersonating as someone else and misusing the access
2.23 Read and adhere to the school policies of e-safety, child protection and anti-bullying
2.24 Be alert and responsible

Tel: 06-5092727 P.O, Box: 45683 Sharjah – U.A.E. www.easuae.com E-mail: info@easuae.com

3. School security systems

3.1 As an effort to maintain network security, integrity and to avoid breach of security, the school ICT department will monitor network activity

3.2 Administrative passwords for the network, servers, school devices, wireless access points are managed confidentially by the ICT department

3.3 All computer devices used by students and staff are connected to the school network and are under regular virus scanning software

3.4 For security and network maintenance purpose, ICT department may monitor devices and network usage at any time

3.5 Sensitive data access is restricted to only those personnel who require access to perform specific duties at school. Access restrictions to such data is maintained by ICT department in conjunction with school Finance department, Human Resource department and Principal.

3.6 **Passwords, Accounts, Data security, and Antivirus** - All school devices are connected with school domain by Windows Active Directory. So, any unauthorized access will not be allowed into the school network. Each authorized user has different password for accessing the school computers. The school Server is secured by **Cisco ASA 5525 x series** firewall control. And the firewall is licensed by Cisco under the UAE regulations. School also has a centralized server-based monitoring with ESET end point security. School is using office 365 mail management system to control the mail filtering and spam controls to their accounts.

Confidential data:

Confidential data is secret and valuable. Common examples are:

- Unpublished financial information.
- Strategies, formulas or new technologies
- Student marks
- Student information
- CCTV recording

All employees are obliged to protect this data.

4. Prohibited use for all users

4.1 Accessing other person's system, account or email

4.2 Visiting unauthorized websites

4.3 Passing any information that is offensive or incorrect

4.4 Violating copyright law

4.5 Sharing passwords or convincing others to share their password

4.6 Deliberately causing harm to other person's work or data

4.7 Intentionally breaching the school's security

4.8 Sharing school's confidential data

4.9 Ignoring e-safety rules

4.10 Using inappropriate language online

4.11 Getting involved in cyber bullying

4.12 Indulging in plagiarism

5. **Consequences of violation of Acceptable ICT Use Policy (Accountability Statement)**: The school reserves the right to take action depending on the severity of violation committed which may include warning, suspension or expulsion but may not be limited to these and may also be involved with reporting the matter with higher authorities.
6. **Declaration by Users**:

☐ I acknowledge that my ward and I have read and fully agree to comply by the Acceptable ICT Use Policy of the school.

☐ I have read and understood the e-safety policy of the school and agree to abide by it.

☐ I understand that any violation of the agreement will result in the loss of the right to use the device/technology as well as may lead to disciplinary action by the school authorities.

☐ We understand that we need to report any concerns/incidents related to e-safety as per the guidelines mentioned in the school e-safety procedure.