مـــدرســـة الـشـــارقـــة الأمريـكـيـة الـدولـيـة
Sharjah American International School

SHARJAH AMERICAN INTERNATIONAL SCHOOL – UMM AL QUWAIN

General E-Safety Policy

Scope of the Policy

This policy applies to all SAIS members (including staff, students, parents) who have access to and are users of schoolIT systems, both in and out of the school.

This policy is related to regulating the behavior of students when they are off the school site and empowering members of staff to impose disciplinary penalties for inappropriate behavior. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place inside or outside of the school but is linked to membershipof the school.

The school will deal with such incidents within this policy and associated behavior and will, where known, inform parents / Caregivers of incidents of inappropriate e-safety behavior that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the SAIS E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

Principal and Online Safety Group:

- The principal has a duty of care for ensuring the e-safety of members of the school community
- The principal and another member of the Safety Committee should be aware of the procedures to befollowed in the event of a serious e-safety allegation being made against a member of staff
- The principal is responsible for ensuring that the E-Safety Leader and other relevant staff

receivesuitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant

- The principal will ensure that there is a system in place to allow for monitoring and support of those inschool who carry out the internal e-safety monitoring role.

Online Safety Group: (Report to the principal)

1. Online Safety Officer Role and Responsibilities:

- Work as the e-safety officer to effectively deliver the e-safety strategy across the school.
- Provide training and resources to staff and students, raising awareness of online safeguarding risks and preventative measures.
- Be aware of potential risks from new and emerging technologies and communicate these to key stakeholders, where appropriate.
- Act as the single point of contact for e-safety issues, liaising with multi-agency partners working with children, young people and other vulnerable people.
- Develop, maintain and quality assure policies and procedures relating to digital technologies and online safeguarding.
- Adhere to new ways of working, embracing change and utilizing new technology.
- Preserve a high degree of confidentiality in respect of customer and personnel information in accordance with the county council's data protection policy.
- Maintain and build good working relationships with colleagues, parents, and students to deliver the service to the required standards.
- Demonstrate awareness/understanding of equal opportunities and other people's behavioral, physical, social and welfare needs.
- Ensure that reasonable care is taken at all times for the health, safety and welfare of yourself and other persons, and to comply with the policies and procedures relating to health and safety.
- Develop an online safety programme for the wider community or to support other schools.
- . Carry out any other duties which fall within the broad spirit, scope and purpose of this job description and which are commensurate with the grade of the post.

2. Students' Roles and Responsibilities:

- Assist the Online Safety Officer in implementing the e-Safety strategy.
- Represent the section they belong to and report all problems to the Online Safety Officer.
- Communicate the Online Safety Group decisions/recommendations to the section of the school to

which they belong.

- Act as digital leaders to raise the awareness and lead others towards fostering an e-safe learningenvironment, actively participate in meetings and assemblies.
- Participate in mentoring programs for new peers to get acquainted with the school policies related to e-safety
- Support their peers in resolving e-safety issues and help them seek the help of the concerned schoolstaff.

3. Teachers' Roles and Responsibilities:

- Assist the Online Safety Officer in implementing the e-Safety strategy.
- Check whether their colleagues are reminding students of the Password Protection Policy.
- Participate in mentoring programs for new peers to get acquainted with the school policies related to e-safety
- Support their peers in resolving e-safety issues and help them seek the help of the concerned schoolstaff.
- Collect all AUP and follow up with teachers and students who are late submitting the required documents.

4. Counselors' Roles and Responsibilities:

- Assist the Online Safety Officer in implementing the e-Safety strategy.
- Schedule awareness campaigns with the help of the Safety Group members for students, parents, andstaff.
- Invite Guest Speakers to discuss Online Safety issues.
- Analyze the Online Incidents Log and submit suggestions for training to Online Safety Officer andPrincipal
- Apply the sanctions for not respecting the Online Safety related Policies and inform the concernedschool staff and parents.
- Hold individual meetings with newly registered students and parents to discuss the school policies andprocedures related to e-safety.
- Clearly communicate and explain the school actions and sanctions for infraction of the school e-safe policies and procedures to all students, parents, and staff, through meetings, assemblies, and school website.

5. Parents' Role and Responsibilities:

- Share the school e-safety strategy with all parents.

- Report parents' concerns to the Online Safety Officer and discuss them during the meetings
- Assist new parents and mentor them to become acquainted with the school e-safety policies andprocedures.

6. IT Technician

The IT Technician will ensure:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required e-safety technical requirements
- That users may only access the networks and devices through a properly enforced password protectionpolicy, in which passwords are regularly changed
- The filtering policy is applied and updated on a regular basis and that its implementation is not thesole responsibility of any single person
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularlymonitored in order that any misuse / attempted misuse can be reported to the principal

Teaching and Support Staff

Are responsible for ensuring that:

- All Teachers have been trained on e-safety and cyberbullying.
- They have read, understood, and signed the Staff Acceptable Use Policy / Agreement
- They report any suspected misuse or problem to the Online Safety Leader or Principal
- All digital communications with students / parents should be on a professional level and only carriedout using official school systems
- Students understand and follow the e-safety and acceptable use policies
- Students have a good understanding of research skills and the need to avoid plagiarism and upholdcopyright regulations
- They monitor the use of the student devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection Officer (Principal) / Safeguarding Designated Safeguarding Lead

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguardingissues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Students:

- Attended awareness workshops on online safety.
- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials andknow how to do so
- Should understand the importance of adopting good e-safety practice when using digital technologies outof school and realize that the school's E-Safety Policy covers their actions out of school, if related to theirmembership of the school

Parents / Caregivers:

Parents / Caregivers play a crucial role in ensuring that their children understand the need to use the internet /mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and caregivers will be encouraged to support the school in promoting good e- safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website

Policy Statements

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognize and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety awareness should be provided as part of teaching.
- Key e-safety messages should be reinforced as part of a planned program of assemblies.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be taught neither to talk to strangers when online nor share personal information such as home address, phone number, etc.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies.
- Students should be encouraged to use school ICT systems in a responsible way, to ensure that there is no risk to their safety or the safety and security of the ICT systems and other users.
- Students should understand that the school will monitor their use of the ICT systems, email and other digital communications.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Students should understand the importance of immediate online incident reporting to the Online Safety Officer or counselors.

- Students should be encouraged to contribute in the school awareness campaigns

Education – Parents

Parents play an essential role in the education of their children and in the monitoring / regulation of the children's on- line behaviors. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet.

The school will provide information and awareness to parents and caregivers through:

- Online parents meeting.
- Messages, flyers, and newsletters on the parents' groups
- Encouraging them to contribute in the school awareness campaigns

Education & Training

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A program of formal e-safety training will be made available to staff. This will be regularly updated andreinforced.
- All new staff should receive e-safety training as part of their induction program ensuring that they fullyunderstand the school e-safety policy and Acceptable Use Agreements
- All e-Safety policies will be presented to and discussed by staff in staff meetings.
- The Online Safety Officer will provide guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering, and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school / academy meets recommendedtechnical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems, and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school / academy technical systems and devices

- The principal is responsible for ensuring that software license logs are accurate and up to date and that regularchecks are made to reconcile the number of licenses purchased against the number of software installations
- Internet access is filtered for all users
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement
- An appropriate system is in place (to be described) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted orotherwise secured.

Bring Your Own Device

The students and the teachers may bring their own laptops as long as they follow these regulations:

- The school has a set of clear expectations and responsibilities for all users
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance

Rent/Buy a School Laptop

Please refer to the Laptop Use Policy for students and the Laptop Use for teachers.

Social Media

Please refer to the social media Policy and Guidelines

Data Protection

Please refer to the Processing of Personal Data Policy and Password Protection Policy

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with and the school actions and sanctions for each type of incident:

Students:

1st Occurrence: A warning letter will be issued by the school to the concerned student. This letter must be signed by both the student and the parent. The student signs an undertaking to abide by the policy or else his/her account will be suspended.

In the event of a second-degree violation, (4 marks) will be deducted
In the event of a third-degree violation, (12) marks will be deducted
In the event of a fourth-degree violation (failure in the behavior subject).

2nd Occurrence: The student's account will be suspended. Parents and students are informed. The student signs an undertaking to abide by the policy or else he will be suspended or expelled.

In the event of a second-degree violation, (8) marks will be deducted
In the event of a third-degree violation, (12) marks will be deducted
In the event of a fourth-degree violation (failure in the behavior subject)

3rd Occurrence: The student will be suspended or expelled; the student will fail the behavior/conduct subject and won't be accepted to register for the next academic year. Legal authorities will be notified.

Important Note: The 3rd occurrence rules might be applied directly, based on the degree of the violation.

Staff:

1st Occurrence: Verbal warning / Written Warning is issued depending on the violation degree.

2nd Occurrence: Final Written warning is issued, the staff member signs an undertaking.

3rd Occurrence: Dismissal from SAIS

This policy was reviewed in August 2021.