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 school IT 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 membership of 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 be followed 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 and reinforced.
- All new staff should receive e-safety training as part of their induction program ensuring that they fully understand 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 recommended technical 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.**

SHARJAH AMERICAN INTERNATIONAL SCHOOL – UMM AL QUWAIN

Data Protection Policy - Parents & Students

Processing of personal data policy

Information memorandum

1. Processing of personal data policy

Sharjah American International School will process your personal data during its activities. This policy sets out the rules that we will follow when processing your personal information to preserve the right to protect your personal data, your privacy, and to ensure that your personal data is not misused. We will follow this policy for the entire period during which we process any of your personal information.

Through this policy, we inform you of the facts and your rights that you need to be aware of, to ensure sufficient transparency in the processing of your personal data.

This policy sets out the procedures and principles on the basis of which we will process and handle your personal data. If anything is unclear or you would like to ask anything about your personal data, please use the contact information provided in this policy.

2. Collection of personal data

2.1. Reasons for collecting personal data

We will only collect and process personal data from you if it is necessary for:

a) Fulfilling the contract that you have signed or closed with us.
b) The provision of the service you want to use.
c) Compliance with the requirements of the law.
d) The purposes of our legitimate interests, unless in this case your interests or the fundamental rights and freedoms of data subjects that require the protection of personal data are preferred.

2.2. Consent

In other cases, we may only collect and process your personal data with your explicit and free consent. You may at any time revoke your consent through the contact details provided in this policy. Specific conditions for the use of your personal data after granting consent are always provided in each individual consent.

2.3. Acquisition of personal data

We do not obtain your personal data from publicly available sources, but always from you or from third parties who cooperate with us and have obtained personal data from you in accordance with the law and may transmit it to us. In both cases, we will follow this policy.

We will always inform you about the specific reason for processing your personal information. This information is either stated directly in the contract, or in the terms of the service provided or in this policy. Alternatively, you may ask us at any time for the reasons for processing your personal information through the contact details listed below.

3. The use of your personal information

We use your personal information primarily to perform a concluded contract, comply with legal requirements, or to meet legal requirements. We will always inform you of any further use of your personal data.

4. Passing your personal information on to others

4.1. Passing on of personal data

We will not share your personal information with anyone except as described in this policy.

Your personal data will be accessed by our employees who will be in charge of working with this personal information. All employees who will have access to your personal data are committed to secrecy in writing; therefore, your personal data may not be disseminated anywhere. These employees are also responsibly selected and properly trained to know how they should treat your personal information and how the processing of your personal data can take place.

We will then pass on your personal information to some third parties if necessary. These persons are referred to as processors. Our company is responsible for ensuring that these processors provide reasonable assurance that your personal data will be processed. We choose all of the processors responsibly. At the same time, the

processors will be contractually obliged to perform all their duties, ensuring that your personal data is adequately protected and minimize the risk of abuse.

4.2. Third persons to whom personal data will be transferred - recipients of personal data

The processors mainly include our accounting, PRO, Corporate Office, and local authorities such as UAQ Education Zone, Ministry of Education, Ministry of Labor, Ministry of Human Resources and Emiratization, Ministry of Health, Technopeak and CTS, our IT partners, Focus, and Insurance Company to whom we pass on your personal information if it is necessary in order to use their services - consultation. Furthermore, IT and hosting providers.

We may also share your personal information with other third parties in order to prevent crime and reduce risks, if required by law and where we consider it appropriate, in response to a lawsuit or to protect the rights or property of our school, our partners or you.

5. Automatic individual decision making and profiling

Our school does not perform any automatic individual decision making or profiling process that would have any legal effect on you or would otherwise have any significant impact on you during the processing of your personal information. If this is changed, we will inform you immediately.

6. Your rights

6.1. Right to information

At any time, you can ask us to send you a confirmation that we are processing some of your personal information at the contact details below and if we are processing your personal data, you have the right to access this information:

a) For what purpose we process your personal data and what its categories are.
b) Who the recipients and processors of your personal data are.
c) How long your personal data will be saved and if this time cannot be determined, then the use criteria to determine this time.
d) Which personal data you may request removal or processing restrictions for and object to such processing.
e) About the right to file a complaint with the Supervisory Authority.
f) About personal data sources, unless they have been obtained from you.
g) Whether automatic decision-making or profiling takes place automatically.

If you ask for it, we will provide you with copies of your processed personal data. If you request it in electronic form, copies will be provided in electronic form if you do not request it in another way. However, we have the right to require verification of your

identity to verify that this information regarding your personal data does not reach an unauthorized person.

Contact Persons are:

Principal (for clarifications or complaints): carole.aboud@saisuaq.com

Assistant Principal (for clarifications or complaints): mona.serhal@saisuaq.com

Heba Abu Taha (School Registrar): heba.abutaha@saisuaq.com

Navas Hussein (Portal Administrator): navas@saisuaq.com

Merouel Brosoto (School Accountant): Merouel.brosoto@saisuaq.com

6.2. The right to correction

 If you find that some of your personal information is inaccurate, imprecise or incomplete, you are entitled to have your personal information corrected or supplemented, without undue delay, after you communicate this fact to us.

7. Measures implemented

Our company has introduced personnel, organizational and technical measures to eliminate the various risks to your rights and freedoms and to protect your personal data. For this purpose, we have trained all of our staff who are in contact with personal data. Furthermore, all personal data in physical form is secured against unauthorized access. For personal data stored in electronic form, we comply with security standards and they are similarly protected against unauthorized access. At the same time, we have developed a risk analysis to prevent risks and have taken appropriate action.

I have read all the points mentioned above and acknowledge that the school is taking all the necessary precautions and measures to safeguard my personal data. I am very well aware that in case of violation of this policy the following sanctions will be applied:

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.

Parent Name: ………………………………..   Student Name: ………………………………..

Parent Signature: …………………………….   Student Signature: ……………………………

SHARJAH AMERICAN INTERNATIONAL SCHOOL – UMM AL QUWAIN

Student/Parent Acceptable Use Policy (AUP)

This policy applies to members of the Governing Body and volunteers as well as external agencies using the ICT systems at Sharjah American International School.

What is an AUP?

We ask all children, young people and adults involved in the life of SAIS to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).
This AUP is reviewed annually, and I will be asked to sign it upon entry to the school and every time changes are made.

Why do we need an AUP?

All staff, governors and volunteers have particular legal / professional obligations, and it is imperative that all parties understand
that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the
school's approaches, strategy and policy as detailed in the full Online Safety Policy, which is available on the school's website.

Where can I find out more?

All staff, governors and volunteers should read SAIS's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behavior Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to School Principal or Online Safety Officer or any Online Safety Team member. Online Safety is considered a safeguarding area. Concerns should be reported in the same way as other Safeguarding concerns.

What am I agreeing to?

1- I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or the safety and security of the ICT systems and other users.

2- I understand that the school will monitor my use of the ICT systems, email and other digital communications

3- I protect my username and password- I will not share it, nor will I try to use any other person's username and password, as mentioned in the SAIS Password Security Policy.

4- I will not talk to strangers when I am communicating online

5- I will not disclose or share personal information about myself or others such as home address, phone number, etc when working online.

6- I will immediately report, as mentioned in the SAIS Reporting Policy, any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to my parents and to either Mr. Youssef, the school Online Safety Officer, or to the school counselors Ms. Ghada or Ms. Oraib.

Yousef.danaf@saisuaq.com

Oraib.mohammad@saisuaq.com

Ghada.abdalla@saisuaq.com

7. I understand that everyone has equal rights to use technology as a resource and:

•   I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so, as mentioned in the SAIS Online Safety Policy.
•   I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
•   I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube).

8. I will act as I expect others to act toward me:
•   I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission, as mentioned in the SAIS Data Protection Policy.
•   I will be polite and responsible when I communicate with others, I will not use strong, aggressive, or inappropriate language and I appreciate that others may have different opinions.
•   I will not take or distribute images of anyone without their permission.

9. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms)

10. I will report any breach of this by others or attempts by pupils to do the same to Mr. Youssef the Online Safety Officer, and/or Ms. Oraib and Ms.Ghada the school counselors.

11. Details on social media behavior, the general capture of digital images/video and on my use of personal devices as stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.

12. I understand the importance of upholding my online reputation, that of the school and of my family, and I will do nothing to impair either.

13. I understand that school systems and users are protected by security, monitoring, and filtering services, so my use of school devices (regardless of time, location or internet connection) and networks/platforms/internet/other technologies, including encrypted content, may be monitored/captured/viewed by these systems and/or relevant/authorized staff members.

14. I will protect my passwords/logins and other access, never share credentials, and immediately change passwords and notify the school's technician.

15. I will not store school-related data on personal devices, storage or cloud platforms. USB Flash drives are not permitted at SAIS for the storage of data.

16. I will only use safe and appropriately licensed software, respecting licensing, intellectual property, and copyright rules at all times.

17. I will use school devices and networks/internet/platforms/other technologies for school business, and I will never use these to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring, will look after devices loaned to me, and will notify the school of "significant personal use".

18. I will not support or promote extremist organizations, messages, or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download, or send material that is considered offensive or of an extremist nature by the school.

19. I understand and support the commitments made by pupil, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.

20. I will install an antivirus and firewall on my personal device to stay protected against viruses and keep them updated.

21. I will not access any link sent to me by an unknown sender. I will visit appropriate website only recommended by either my teachers or my parents.

21. I understand that I am given appropriate access to my role and relationship within the school. If I discover my settings are incorrect, I will inform the school's senior leadership team immediately

22. I will not deliberately attempt to access content that I do not require in order to fulfil my role with the school

23. I will strictly follow the Plagiarism Policy Guidelines and respect Intellectual Propriety and Copyrights Rights.

SHARJAH AMERICAN INTERNATIONAL SCHOOL – UMM AL QUWAIN

Parent Acceptable Use Policy Agreement

By signing this document, you confirm that you have read, understood, and agreed to all the points addressed in this agreement.
I understand that it is my responsibility to ensure I remain up to date and understand the school's most recent online safety/ safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Parent Name: _____

Relationship to Student: _____

Signature: _____   Date: _____

Student Name:	*Class:*
Students' Acceptable Use Agreement	

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)

- I use my own equipment in school (when allowed)

- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, VLE, website etc.

- I understand that network and Internet access may be monitored.

- I am well aware that the consequences of violation of the Online Safety Policy are:

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.

Student Name: (write your name please):
………………………………………………………..

Date: ………………………………………………………………

This agreement was reviewed in August 2021.

Sharjah American International School (SAIS)–Umm Al Quwain Campus

Password Protection Policy –Elementary Students

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All SAIS students are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

3. Scope

The scope of this policy includes all SAIS users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any SAIS facility, has access to the SAIS network, or stores any non-public SAIS information.

4. Policy

4.1 Password Creation

4.1.1 All students' passwords must conform to the ==*Password Construction Guidelines*.==

4.1.2 Users must use a separate, unique password for each of their work-related accounts. Users may not use any school related passwords for their own, personal accounts.

4.2 Password Change

4.2.1 Passwords should be changed every month.

4.2.2 Passwords may not be written down.

4.3 Password Protection

4.3.1 Passwords should be treated as confidential information. No student is to give, tell, or hint at their password to another person, including Technology staff, administrators, supervisors, classmates, friends, and family members, under any circumstances. If someone demands your password, refer them to this procedure or have them contact the Technology Department or their

teacher/supervisor. Exception: Students can share their passwords with their parents/guardians and are encouraged to do so.

4.3.2. Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to district resources via the District's IPsec-secured Virtual Private Network or SSL-protected Web site.

4.3.3 No user is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in an encrypted file if in electronic form.

4.3.4 Students should not use the "Remember Password" feature of applications (for example, webbrowsers).

4.3.5 If a student either knows or suspects that his/her password has been compromised, it must bereported to the Online Safety Group and the password changed immediately.

4.3.5 The IT Department may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of theseaudits, the user will be required to change his or her password immediately

5. Password Reset Procedure

Students should contact Mr. Kumar, the IT technician or Mr. Youssef, the Online Safety Officer. The request will be followed up with a return call (if the user is not their physically) to validate the user requesting the change. Upon validation, the password will be set to a new unique password and read over the phone to the user while they are logging in. Passwords are not to be sent via e-mail. Students will be asked to change the password immediately after the reset is done successfully.

6. Policy Compliance

5.1 The Compliance Measurement

The IT Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru, video monitoring, internal and external audits, and feedback tothe principal.

5.2 Exceptions

Any exception to the policy must be approved by the IT Department in advance.

5.3 Non-Compliance

A student found to have violated this policy may be subject to disciplinary action, up to andincluding being suspended.

7. Password Construction Guidelines

1. Passwords must contain at least 8 characters.

2. Passwords must contain both upper- and lower-case letters.

3. Passwords must contain at least one number (for example, 0-9).

4. Passwords must contain at least one special character (for example,$%^&*()_+|~-=\`{}[]:";'<>?,/).

5. Passwords should not be found in a dictionary

6. Passwords should not contain personal information such as birthdates, addresses, phonenumbers, or names of family members, pets, friends, and fantasy characters.

I have read, understood, and will abide by the Password Protection Policy. I further understand that any violation of this policy may be subject to disciplinary action, up to and including being suspended/expelled.

1st Occurrence: A warning letter will be issued by the school to the concerned student. This letter should be signed by both student and parent. The student signs an undertaking to abide by the policy or else his account will be suspended. 6 behavior marks are deducted.

2nd Occurrence: The student's account will be suspended. The student signs an undertaking to abide by the policy or else he will be suspended. 12 behavior marks are deducted.

3rd Occurrence: The student will be suspended. The student will fail the behavior/conductsubject. Legal Authorities will be notified

Username

_____

User Signature

_____

This policy was reviewed in August 2021.

Sharjah American International School (SAIS)–Umm Al Quwain Campus
ICT Acceptable Use Policy
Elementary Student's Agreement / Password Security Policy

This is how I will protect my password:

I will follow the school Password Construction Guidelines to create a strong password

I will change my password every month.

I will not share my password with anyone, except my parents.

I will contact Mr. Kumar or Mr.Youssef if I want my password to be reset.

I will immediately inform the Online Safety Group if I suspect my password has been compromised. I will immediately change my password.

I have read, understand, and will abide by the Password Protection Policy. I further understand that any violation of this policy may be subject to disciplinary action, up to and including being suspended.

1st Occurrence: A warning letter will be issued by the school to the concerned student. This letter should be signed by both student and parent. The student/guardian signs an undertaking to abide by the policy or else the student's will be suspended. 6 behavior marks will be deducted for grade 3 & 4 students.

2nd Occurrence: The student's account will be suspended. 12 behavior marks will be deducted for grade 3 & 4 students.

3rd Occurrence: The student will be suspended. The student will fail the behavior/conduct subject. Legal Authorities will be notified.
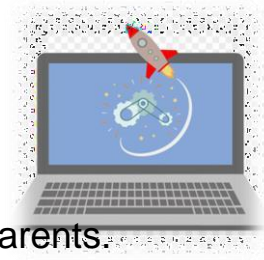
.... [Print child's name] agrees to follow the Password Protection Policy

Signed…………………………………………

Class ……………………………………………….

Date………………………………………
This agreement was reviewed in August 2021.

Sharjah American International School (SAIS)–Umm Al Quwain Campus

Password Protection Policy – Middle & High School Students

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All SAIS students are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

3. Scope

The scope of this policy includes all SAIS users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any SAIS facility, has access to the SAIS network, or stores any non-public SAIS information.

4. Policy

4.1   Password Creation

4.1.1 All students' passwords must conform to the *Password Construction Guidelines*.

4.1.2 Users must use a separate, unique password for each of their work related accounts. Users may not use any school related passwords for their own, personal accounts.

4.2   Password Change

4.2.1 Passwords should be changed every month.

4.2.2 Passwords may not be written down, unless stored in an encrypted format.

4.3   Password Protection

4.3.1 Passwords should be treated as confidential information. No student is to give, tell, or hint at their password to another person, including Technology staff, administrators, supervisors, classmates, friends, and family members, under any circumstances. If someone demands your password, refer them to this procedure or have them contact the Technology Department or their teacher/supervisor. Exception: Students can share their passwords with their parents/guardians and are encouraged to do so.

4.3.2. Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to district resources via the District's IPsec-secured Virtual Private Network or SSL-protected Web site.

4.3.3 No user is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in an encrypted file if in electronic form.

4.3.4 Students should not use the "Remember Password" feature of applications (for example, web browsers).

4.3.5 If a student either knows or suspects that his/her password has been compromised, it must be reported to the Online Safety Group (by email or on Teams) and the password changed immediately.

4.3.5 The IT Department may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately

5. Password Reset Procedure

Students should contact Mr. Kumar, the IT technician or Mr. Youssef, the Online Safety Officer. The request will be followed up with a return call (if the user is not their physically) to validate the user requesting the change. Upon validation, the password will be set to a new unique password and read over the phone to the user while they are logging in. Passwords are not to be sent via eMail. Students will be asked to change the password immediately after the reset is done successfully.

6. Policy Compliance

5.1 Compliance Measurement

The IT Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru, video monitoring, internal and external audits, and feedback to the principal.

5.2 Exceptions

Any exception to the policy must be approved by the IT Department in advance.

5.3 Non-Compliance

A student found to have violated this policy may be subject to disciplinary action, up to and including being suspended or expelled.

1st Occurrence: A warning letter will be issued by the school to the concerned student. This letter should be signed by both student and parent. The student signs an undertaking to abide by the policy or else his account will be suspended. 6 behavior marks are deducted.

2nd Occurrence: The student's account will be suspended. The student signs an undertaking to abide by the policy or else he will be suspended. 12 behavior marks are deducted.

3rd Occurrence: The student will be suspended. The student will fail the behavior/conduct subject. Legal Authorities will be notified.

7. Password Construction Guidelines

Passwords are used to access the network, Teams, e-mail, the Web, and voicemail.

Poor, weak passwords are easily cracked, and put the entire system at risk. Therefore, strong passwords are required. Try to create a password that is also easy to remember.

1. Passwords must contain at least 8 characters.

3. Passwords must be at least 8 characters in length and contain characters from three of the four following categories: Sample: We1come! (Do not use this sample)

a. English uppercase characters (A through Z)

b. English lowercase characters (a through z)

c. Base 10 digits (0 through 9)

d. Non-alphabetic characters (for example, !, $, #, %)

4. Passwords may not contain your First, Middle or Last name

5. Passwords should not be based on well-known or easily accessible personal information suchas date of birth or phone number.

6. Passwords should not be words that can be found in a standard dictionary (English or foreign) or are publicly known slang or jargon.

Password Creation Tips:

1. Think of a sentence that you can remember. This will be the basis of your strong password or pass phrase. Use a memorable sentence, such as "My son Age is three years old."

2. Check if the computer or online system supports the pass phrase directly. If you can use a passphrase (with spaces between characters) on your computer or online system, do so.

3. If the computer or online system does not support pass phrases, convert it to a password. Take the first letter of each word of the sentence that you've created to create a new, nonsensical word. Using the example above, you'd get: "msaityo".

4. Add complexity by mixing uppercase and lowercase letters and numbers. It is valuable to use some letter swapping or misspellings as well. For instance, in the pass phrase above, consider misspelling Aiden's name, or substituting the word "three" for the Procedure: 6800.6P Page 4 of 4 number 3. There are many possible substitutions, and the longer the sentence, the more complex your password can be. Your pass phrase might become "My SoN Ayd3N is 3 yeeRs

old." If the computer or online system will not support a pass phrase, use the same technique on the shorter password. This might yield a password like "MsAy3yo".

5. Finally, substitute some special characters. You can use symbols that look like letters, combine words (remove spaces) and other ways to make the password more complex. Using these tricks, we create a pass phrase of "MySoN 8N i$ 3 yeeR$ old" or a password (using the first letter of each word)

I have read, understand, and will abide by the above Policy. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be initiated.

1st Occurrence: A warning letter will be issued by the school to the concerned student. This letter should be signed by both student and parent. The student signs an undertaking to abideby the policy or else his account will be suspended. 6 behavior marks are deducted.

2nd Occurrence: The student's account will be suspended. The student signs an undertaking to abide by the policy or else he will be suspended. 12 behavior marks are deducted.

3rd Occurrence: The student will be suspended. The student will fail the behavior/conduct subject. Legal Authorities will be notified.

User Name

_____

User Signature

_____

This policy was reviewed in August 2021.

Sharjah American International School (SAIS)–Umm Al Quwain Campus

ICT Acceptable Use Policy
Middle/High School Student's Agreement / Password Security Policy

This is how I will protect my password:

I will follow the school Password Construction Guidelines to create a strong password

I will change my password every month.

I will not share my password with anyone, except my parents.

I will contact Mr. Kumar or Mr. Youssef if I want my password to be reset.

I will immediately inform the Online Safety Group if I suspect my password has been compromised. I will immediately change my password.

I have read, understood, and will abide by the Password Protection Policy. I further understand that any violation of this policy may be subject to disciplinary action, up to and including being suspended/expelled.

1st Occurrence: A warning letter will be issued by the school to the concerned student. This letter should be signed by both student and parent. The student signs an undertaking to abide by the policy or else his account will be suspended. 6 behavior marks are deducted.

2nd Occurrence: The student's account will be suspended. The student signs an undertaking to abide by the policy or else he will be suspended. 12 behavior marks are deducted.

3rd Occurrence: The student will be suspended. The student will fail the behavior/conduct subject. Legal Authorities will be notified.

.... [Print student's name] agrees to follow the Password Protection Policy

Signed…………………………………………

Class ....
Date...

SHARJAH AMERICAN INTERNATIONAL SCHOOL – UMM AL QUWAIN

Internet Use Monitoring and Filtering Policy - Student

1. Purpose

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within SAIS's network. These standards are designed to ensure students use the Internet in a safe and responsible manner and ensure that student web use can be monitored or researched during an incident.

2. Scope

This policy applies to all SAIS students connected to the SAIS network.
This policy applies to all end user-initiated communications between SAIS's network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

3. Policy

3.1 Web Site Monitoring

The Information Technology Department shall monitor Internet use from all computers and devices connected to the corporate network. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 180 days.

3.2 Access to Web Site Monitoring Reports

General trending and activity reports will be made available to any student as needed upon request to the Information Technology Department. Computer Security Incident Response Team (CSIRT) members (Mr. Kumar) may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the CSIRT upon written or email request to Information Systems from a Human Resources Representative.

3.3 Internet Use Filtering System

The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for SAIS's corporate environment. The following protocols and categories of websites should be blocked:

• Social Network Services •Personals and Dating • SPAM, Phishing and Fraud • Spyware • Tasteless and Offensive Content • Violence, Intolerance and Hate • Web Based Email • Peer to Peer File Sharing	• Adult/Sexually Explicit Material • Advertisements & Pop-Ups • Chat and Instant Messaging • Gambling • Hacking • Illegal Drugs • Intimate Apparel and Swimwear

3.4 Internet Use Filtering Rule Changes

The Information Technology Department shall periodically review and recommend changes to web and protocol filtering rules. Human Resources shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Policy.

3.5 Internet Use Filtering Exceptions

If a site is mis-categorized, students may request the site be un-blocked by submitting a ticket to the school principal. The principal will review the request and request to un-block the site if it is mis-categorized.

Students may access blocked sites with permission if appropriate and necessary for business purposes. If a student needs access to a site that is blocked and appropriately categorized, they must submit a written request to the school principal. The principal will present all approved exception requests to Information Technology in writing or by email. Information Technology will unblock that site or category for that associate only. Information Technology will track approved exceptions and report on them upon request.

4. Policy Compliance

5.1 Compliance Measurement

The Online Safety Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits.

5.2 Exceptions

Any exception to the policy must be approved by the school principal.

5.3 Non-Compliance

A student found to have violated this policy may be subject to <u>disciplinary action</u>.

I have read, understand, and will abide by the above Policy. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action may be initiated, as following:

1st Occurrence: A warning letter will be issued by the school to the concerned student. This letter must besigned 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, (4marks) 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. Thestudent 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 deductedIn 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/conductsubject, 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 theviolation.

Parent Name: …………………………………..   Student Name: ……………………………

Parent Signature: …………………………………   Student Signature: ……………………………

Online Safety Incidents

Reporting Policy-Students

Online Safety is being aware of the nature of the possible threats that you could encounter whilst engaging in activity through the Internet, these could be security threats, protecting and managing your personal data, online reputation management, and avoiding harmful or illegal content.

By practicing Online Safety, we can prevent and mitigate the risks that are inherently involved with using digital technologies, platforms, and services.

Online Safety Incidents include but are not limited to:

• unwanted contact/content

• social exclusion

• threats and abuse

• damage to reputation

• fraud and viruses

• lack of consent

As per Article 21 of the UAE Federal Decree Law 5/2012, cybercrimes are punishable by a jail term of at least six months and/or a fine not less than Dh150,000 and not exceeding Dh500,000.

HOW TO REPORT ONLINE SAFETY INCIDENTS?

1. **Take screenshots** and save everything related to the incident.   Make sure this includes text, images, dates, times, handles, and descriptions.

2. **Block and report the per**son/post.

SHARJAH AMERICAN INTERNATIONAL SCHOOL – UMM AL QUWAIN

3. **Call the school hotline 0564808233.**

4. **Report** the incident **immediately** to your parents and to Mr. Yousef, the Online Safety Officer or the school counselors Ms. Ghada or Ms. Oraib on the following emails:

> yousef.danaf@saisuaq.com
>
> oraib.mohammad@saisuaq.com
>
> Ghada.abdalla@saisuaq.com

5. **Report to police on 999, or online at www.ecrime.ae, 80012, or Interior Ministry toll free number 116111.**

6. You can also **report anonymously** incidents through the School Drop Box at the reception or "Reporting Center" on Teams.

WHAT ARE THE DISCIPLINARY ACTIONS OF THE ONLINE SAFETY INCIDENTS?

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)

SHARJAH AMERICAN INTERNATIONAL SCHOOL – UMM AL QUWAIN

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.

Parent Name: ………………………………..
…………………………………..

Student Name:

Parent Signature: ………………………………
…………………………………

Student Signature:

SHARJAH AMERICAN INTERNATIONAL SCHOOL – UMM AL QUWAIN

Social Media Policy and Guidelines- Student

1. Introduction

We actively encourage the responsible use of social media. Responsible use of social media can be positivefor learning and teaching. It can also be personally enjoyable and beneficial.

This policy will make clear what standards are expected of anyone who works for the school and uses socialmedia as well as what actions may be taken when it is considered a student may have breached thispolicy.

1.1   This policy applies to all student use of social media, including:

      1.1.1   on behalf of the school.

      1.1.2   as part of their work directly with pupils.

      1.1.3   In their wider professional lives; and

      1.1.4   In their personal lives.

1.2   There is additional guidance available to help student follow good practice on the e-safety toolkit area of the social media.

1.3   In this policy, we define **social media** to mean:

      'Websites and applications that enable users to create and share content or to participate in socialnetworking.'

1.4   In this policy, the word **parents** is used to mean the parents, care-givers, and others with parentalresponsibility for a pupil at the school.

1.5   This policy works alongside other legislation, DFE statutory guidance, and other school and localauthority policies such as Code of student Conduct, Online Safety Policy and Acceptable use agreement. These all also apply where relevant.

2. PURPOSE

This policy has been created to assure that information disclosed by SAIS and its students' is timely, accurate, comprehensive, authoritative, and relevant to all aspects of school's system. In accordance with the SAIS Belief Statement that there must be a clear alignment among curriculum, instructional practice and assessment, this policy will provide the framework to facilitate the timely dissemination of information.

(a)   Adherence to this policy will reinforce its current non- discriminatory practices based onsex, race, color, national origin, religion, handicap, age, or disability.

clarify what the school considers to be appropriate and inappropriate use of socialnetworking by student.

(b)   encourage social networking to be used in a beneficial and positive way,

(c)   safeguard student, pupils, parents, and members of the public from abuse through socialnetworking,

(d)   safeguard the reputation of the school, other schools, other organizations, and employersfrom unwarranted abuse through social networking,

(e)   set out the procedures that will be followed where it is considered that student haveinappropriately or unlawfully used social networking.

3. SCOPE

This social media policy applies to all SAIS employees, teachers, students, Board Members, and auxiliary personnel. This policy covers all social media and media platforms, social networks, blogs, photo sharing, wikis, online forums, and video sharing.

4. DEFINITIONS

Term: Social Media Account
Definition: A personalized presence inside a social networking channel, initiated at will by an individual.YouTube, Twitter, Facebook, Instagram, Snap Chat, and other social networking channels allow users to sign-up for their own social medial account, which they can use to collaborate, interact, and share contentand status updated. When a user communicated through a social media account, their disclosures are attributed to their User Profile.

Term: Social Media Channels
Definition: Blogs, micro-blogs, wikis, social networks, social bookmarking services, user rating servicesand any other online collaboration, sharing or publishing platform, whether accessed through the web, a mobile device, text messaging, email or other existing or emerging communications platforms.

Term: Professional social media
Definition: Professional social media is a work-related social media activity that is either school based(e.g. establishing a Facebook page for school, school department), or non-school based.

Term: Social Media Disclosures
Definition: Blog posts, blog comments, status updated, text messages, posts via email, images, audiorecordings, video recordings or any other information made available through a social media channel.Social media disclosures are the actual communications a user distributes through a social media channel, usually by means of their social media account.

Term: Controversial Issues
Definition: Issues that form the basis of heated debate, often identified in political campaigns as wedge issues, since they provoke a strong emotional response. Examples include political views, health care reform,education reform and gun control.

Term: Inbound Links
Definition: An inbound link is a hyperlink that transits from one domain to another. A hyperlink that transits from an external domain to your own domain is referred to as an inbound link. Inbound links areimportant because they play a role in how search engines rank pages and domains in search results.

Term: Hosted Content
Definition: Text, pictures, audio, video, or other information in digital form that is uploaded and resides inthe social media account of the author of a social media disclosure. If you download content off the Internet, and then upload it to your social media account, you are hosting that content. This distinction is important because it is generally illegal to host copyrighted content publicly on the Internet without first obtaining the permission of the copyright owner.

Term: Copyrights
Definition: Copyrights protect the right of an author to control the reproduction and use of any creative expression that has been fixed in tangible form, such as literary works, graphical

works, photographic works, audiovisual works, electronic works and musical works. It is illegal to reproduce and use copyrighted content publicly on the Internet without first obtaining the permission of the copyright owner.

Term: Official Content
Definition: Publicly available online content created and made public by SAIS, verified by virtue of the fact that it is accessible through the school's website.

Term: Blog
Definition: An online journal that contains entries or posts that consist of text, links, images, video, or other media and is
usually between 300-500 words.

Term: Microblogging
Definition: Posting brief and often frequent updates online. Unlike traditional blogs, which are often hosted on a custom website, microblogs are typically published on social media sites like Twitter, Instagram, Tumblr, and Facebook.

Term: Cyberbullying
Definition: Cyberbullying is the use of electronic information and communication devices, to include but not limited to email messages, instant messaging, text messaging, cellular telephone communications, Internet blogs, Internet chat rooms, Internet postings and defamatory websites.

5. **FACULTY AND STUDENT GUIDELINES**

  Blogs, Wikis, Podcasts, Digital

  Images & VideoPersonal

  Responsibility

students are personally responsible for the hosted content they publish online. Be mindful that what you publish on social media channels will be public for a long time protect your privacy. When posting online, please remember that you are a student of the SAIS and representative of your colleagues, students, parents, and the school community.

Your online behavior should reflect the same standards of honesty, respect, and consideration that you use face-to-face.

Blogs, wikis, and podcasts are an extension of your classroom and considered *official content*. What is inappropriate in the classroom should be deemed inappropriate online.

Do not post photos or movies of fellow students without their permission. Do not use photos or movies taken at school without permission. Do not post photos or movies that contain students without parental consent.

There are many websites that allow users to share personally created movies. You are responsible forall you do, say and post online including videos. Anything posted online should represent you in a professional manner as others will see you as connected to SAIS. It disrupts learning when teachers, employees, and student post videos with questionable content.

When posting online be sure not to post confidential student information.

Cyberbullying is not to be tolerated. Any incidence of cyberbullying should be reported to the school**Principal and Online Safety Officer** immediately. All cyberbullying incidents are to be taken seriously.

Personal use of social networking site, including Facebook, Twitter, and Instagram

Student and employees are personally responsible for all comments/information and hosted content they publish online. Be mindful that things such as *Tweets* and *Status Updates* will be visible and public for a long time.

By posting comments, having online conversations, etc. on social media sites you are broadcastingto the world, be aware that even with the strictest privacy settings, what you 'say' online should bewithin the bounds of professional discretion. Comments expressed via social networking pages under the impression of a 'private conversation' my still end up being shared into a more public domain, even with privacy settings on maximum.

Comments related to SAIS, its employees, student and/events related to SAIS, should always meet the highest standards of professional discretion. When posting, even on the strictest settings, student shouldact on the assumption that all postings are in the public domain.

Before posting photographs and videos, permission should be sought from the subject where possible. This is especially the case where photographs of professional colleagues are concerned.

Before posting personal photographs, thought should be given as to whether the images reflect on your professionalism.

Photographs relating to alcohol or tobacco use may be deemed inappropriate. Remember, your socialnetworking site is an extension of your personality, and an extension of your professional life and classroom. If it would seem inappropriate to put a certain photograph on the wall, then it should be considered inappropriate to post online.

Microblogging (Twitter, Facebook, Tumblr, Instagram, etc.) comments made using such media are not protected by privacy settings. students should be aware of the public and widespread nature of such media and refrain from any comment and/or #hashtags that could be deemed unprofessional. #(Hashtags) that tag students and provide personal financial gain are prohibited. SAIS students are not to be used as a promotional audience.

SAIS students are not permitted to solicit or accept "Friend" Requests from SAISemployees on any personal Social Media Account. This includes student's accounts and SAIS employee personal accounts.

6. **Managing Procedure for posting videos and pictures on the school social media accounts**

   SAIS has 2 social media accounts:

1. Facebook Account (IT Teacher responsible for posting: To be announced)
2. Instagram Account (IT Teacher responsible for posting: Heba AlTahawy)
3. Whatsapp Groups as a one-way communication with parents (Coordinators are the only members who canpost information)
4. Class Dojo is used by KG and Elementary Teachers

1 & 2: Student members, wishing to post videos or pictures on the school's social media accounts, should email their contribution to the concerned section coordinator responsible for the grade level, to which the post is related.

The section coordinator will then check the content of the videos and pictures, ensure that all students included in the videos and pictures have already submitted the consent letters signed by their parents to have them on the school social media accounts. (Each section coordinator saves all the consent letters in a folder onhis/her workstation).

Once the checking is done, the coordinator will forward the email to Ms. Heba to post on theschool social media accounts.

3.   Section Coordinators post all information related to the hybrid learning environment on these groups. Theyare the only ones allowed to post information.

4.   Class Dojo is used by KG and Elementary teachers as a means of communication with parents concerningtheir children's performance.

7. Student-Student Relations

Students are prohibited from establishing personal relationships with employees that are unprofessional and thereby inappropriate. Examples of unprofessional relationships include, butare not limited to: employees fraternizing or communicating with students as if employees and students were peers such as writing personal letters or emails; "texting" students; calling students on cell phones or allowing students to make personal calls to them unrelated to homework or class work; sending inappropriate pictures to students; discussing or revealing to students personal matters about their private lives or inviting students to do the same.

Students who post information on Facebook, Twitter or other similar websites that include inappropriate personal information such as, but not limited to: provocative photographs, sexually explicit messages, use of alcohol, drugs or anything students are prohibited from doing must understand that if students, parents obtain access to such information, their case will be investigated by school and authorities and if warranted, will be disciplined up to andincluding termination, depending on the severity of the offense.

The principal reserves the right to periodically conduct Internet searchers to determine if students have posted inappropriate materials online. If inappropriate use of computers and websites is discovered, the principal will download the offensive material and promptly bringmisconduct to the attention of the COO.

8. Email

SAIS in accordance with its **Acceptable Use and Safety** policy, that all electronic or any othercommunications by students or parents to employee at any time, from any email system shall be expected to be professional, acceptable in content to any reasonable person, and limited to information that is school-related or is acceptable to both student and parent. Email between employees, students, and parents shall be done through the school provided email application. Email must conform to school email policies.

9. CYBERBULLYING:

Cyberbullying by a SAIS student directed toward another SAIS student or school student member isconduct that disrupts both a pupil's ability to learn and a school's ability to educate its pupils in asafe environment.

SAIS prohibits acts of cyberbullying by SAIS students through the use of any SAIS owned, operated, and supervised technologies. The school principal or designee may report allegationsof cyberbullying to law enforcement authorities.

Any act online, the Internet or through electronic devices (cellular phones, tablets) that deliberately threatens, harasses, intimidates an individual or group of individuals; places an individual in reasonable fear of harm to the individual or damage to the individual's property;has the effect of substantially disrupting the orderly operation of the school is considered cyberbullying.

Any student that believes he/she has or is being subjected to cyberbullying, as well as any person who has reason to believe a student or school student member has knowledge or reason to believe another pupil or school student member is being subjected to orhas been subjected to cyberbullying shall immediately make a report to the school principal and Online Safety Officer.

SAIS has a zero tolerance against cyberbullying and each reported instance will be handledin accordance with the UAE rules, policies, and guidelines.

10. MEDIA, PHOTOGRAPHY AND FILM

A reporter, producer or other news media may contact you for a number of reasons, for example:

To get information about SAIS, teachers, or employees or students.

To get information about a recent, unexpected event such as natural disasters, theftsor arrests, accidents, or injuries; parent or teacher complaints; etc.

To get information or comments about an action or event that could impact our school, teachers and/or student, students or changes in school or government policies.
To get general information on a topical story in our community.

Refer all media calls to your school's *Principal*. Please do not say you are not allowed to talkto a reporter or have to get permission to do so. Instead, tell the reporter: "SAIS policy is to refer all media inquiries to the principal."

Please remember to contact your school's *Principal* if and when you have been approachedby the media. Even though you have referred the media, the principal will need to prepare aresponse. Do not let a reporter compel you to answer questions on the spot. It is always beneficial to prepare in advance in order to provide accurate and relevant information.

A similar process as described above will be used when someone from the media is requesting permission to take photographs or to film inside one of our facilities. Refer thecaller to your school's Principal. No one will be given access to your facility/school for a photo or filming without approval from the principal and equally important the principal willnot give approval without talking in advance with the COO.

11. Monitoring use of social media on school equipment

• The school reserves the right to monitor **all** student internet use, including when student are making personaluse of social media, on any school systems or equipment. Misuse of social media – even personal use –on school equipment is a breach of the school's acceptable use policy.

12. BLOGGING GUIDELINES AND BEST PRACTICES

SAIS continues to explore how online discourse through social media channels can empower teachers, students, parents, and student. SAIS understands the importance of these interactions in helping to communicate the highlights of academic collaboration and achievement. SAIS is committed to continuing to explore new technologies and their bestpractices.
These Blogging Guidelines and Best Practices will help you to make appropriate decision about your SAIS-related blogging, blog content curation, and your responses to comments and blogs. The lines between public and private, personal, and professional are often blurred in the digital world.

By virtue of identifying yourself as a SAIS student online, you are now connected to colleagues, students, parents, and the school community. You should make sure that contentassociated with you is consistent with your work at SAIS.

All blogs and other media will be posted at the discretion of each school 's Principal. Anyblog or other social media involving SAIS can be posted and/or removed at the principal'sdiscretion.

All blogs and other social media sites are a communication channel of SAIS and are to bemaintained consistently throughout the school year.

SAIS students are personally responsible for the content they publish online. Be mindful that what you publish will be public for a long time. Remember to protect yourprivacy.

As with all online interaction, as a SAIS student your online behavior should reflectthe same standards of honesty, respect, and consideration that you use face-to-face.
Remember that blogs are an extension of your classroom. What is inappropriate in yourclassroom should be deemed inappropriate online.

You may not share information that is confidential and proprietary about SAIS, itsemployees, students and/or student.

When blogging, be respectful of your colleagues. Be thoughtful and accurate in your writing,and respectful of how other SAIS members may be affected.

Remember that blogs are *brief* and should not exceed more than 500 words. Be concise andknow your audience.

When blogging online, do not post confidential student information, including grades, awards and/or disciplinary action. If you are unsure of what is considered confidential, contact your school's Principal.

SAIS students should include disclaimers within their personal blogs that the viewsare their own and do not reflect on SAIS.

Classroom blogs do not require a disclaimer, but teachers are encouraged to moderate content contributed by students.

Remember to respect copyright and fair use guidelines. Be sure not to plagiarize and givecredit when it is due.

Blogs and comments related to SAIS should always meet the highest standards of professional discretion. When posting or blogging, even on the strictest settings, student shouldact on the assumption that all postings are in the public domain.

I have read, understand, and will abide by the above Policy. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may betaken, and/or appropriate legal action may be initiated, as per the following:

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.

Parent Name: ………………………………..
………………………………..   Student Name:

Parent Signature: ………………………………   Student Signature:

. . . .

Sharjah American International School (SAIS)

Guest (Host) Acceptable Use Policy (AUP)

What is an AUP?

We ask all children, young people and adults involved in the life of SAIS to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).
This AUP is reviewed annually, and I will be asked to sign it upon entry to the school and every time changes are made.

Why do we need an AUP?

All staff, governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy, which is available on the school's website.

Where can I find out more?

All staff, governors and volunteers should read SAIS's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Reporting Policy, Data Protection Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to School Principal or Online Safety Officer or any Online Safety Team member. Online Safety is considered a safeguarding area. Concerns should be reported in the same way as other Safeguarding concerns.

Terms and conditions for SAIS staff member sponsoring guest access

1. You are responsible for maintaining the confidentiality of your password and all activities that occur under your username and password. SAIS offers this service so that you can sponsor guests for WiFi access on campus. If your guests violate any of the terms and conditions below, as the sponsor, you will be held accountable and will face the relevant disciplinary procedures established for staff at SAIS.

2. Upon gaining WiFi access, your guests may browse the World Wide Web and access other internet-dependent technologies. However, guests must comply with the Policy and Rules on Internet and Email Use. Additionally, guests may not perform high volume data transfers – especially sustained high volume data transfers. They may not host a web server or any other server. Guests may not interfere with other network users, attempt to access someone else's account, send unsolicited bulk email, or collect other people's personal data without their knowledge.

3. SAIS reserves the right to suspend the service if reasonably believes that you or your guest are using the service for criminal or illegal activities, making unreasonably excessive use of the service, or otherwise violating SAIS policies and agreements. SAIS reserves the right to revise, amend or modify these Terms and Conditions, or other policies and agreements, and aspects of the service itself.

4. I have read and understood SAIS's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behavior as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.

I understand it is my duty to support a whole-school safeguarding approach and will report any behavior which I believe may be inappropriate or concerning in any way to Mr. Yousef Al Danaf, the Online Safety Officer, reachable at
yousef.danaf@saisuaq.com

6.I understand the responsibilities listed for my role in the school's Online Safety policy and agree to abide by these.

1- You are responsible for maintaining the confidentiality of your password and all activities that occur under your username and password. SAIS offers this service so that you can browse the World Wide Web and access other internet-dependent technologies. If you violate any of these terms and conditions, you will be held responsible. Additionally, the person who sponsored your access will also be held accountable and will face the relevant disciplinary procedures established for staff at SAIS. You may not share this service with a third party.

2- By accepting these terms and conditions, you agree to comply with the Policy and Rules on Internet and Email Use.

3- Additionally, you may not perform high volume data transfers – especially sustained high volume data transfers. You may not host a web server or any other server. You may not interfere with other network users, attempt to access someone else's account, send unsolicited bulk email, or collect other people's personal data without their knowledge.

4- **SAIS reserves the right to suspend the service and/or report the user to the relevant authorities** if SAIS reasonably believes that you are using the service for criminal or illegal activities, making unreasonably excessive use of the service, or otherwise violating SAIS policies and agreements. SAIS reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the service itself.

مــدرســة الـشــارقــة الأمـريـكـيـة الـدولـيـة
Sharjah American International School

Sharjah American International School (SAIS)

Guest/Staff Acceptable Use Policy Agreement

By signing this document, you confirm that you have read, understood and agreed to the 20 points addressed.

I understand that it is my responsibility to ensure I remain up to date and understand the school's most recent online safety/ safeguarding policies. I understand that failure to comply with this agreement will lead to suspension of the service and reporting to relevant authorities.

Guest Name: _____

Staff Hosting guest: _____

Staff Signature:_____

Guest Signature:_____

Date: _____

This policy was reviewed in August 2021.