المدرسة السويسرية الدولية

SWISS INTERNATIONAL SCHOOL
QATAR

ACCEPTABLE USE POLICY (IT POLICY)

Staff Incharge	IT Officer & IT Integrator
Latest revision	September 2025
Approved by	Head of School
Next Revision	September 2026

المدرسة السويسرية الدولية

SWISS INTERNATIONAL SCHOOL
QATAR

Our Vision

SISQ aims to develop learners who are

FULFILLED INSPIRED PREPARED

رؤيتنا

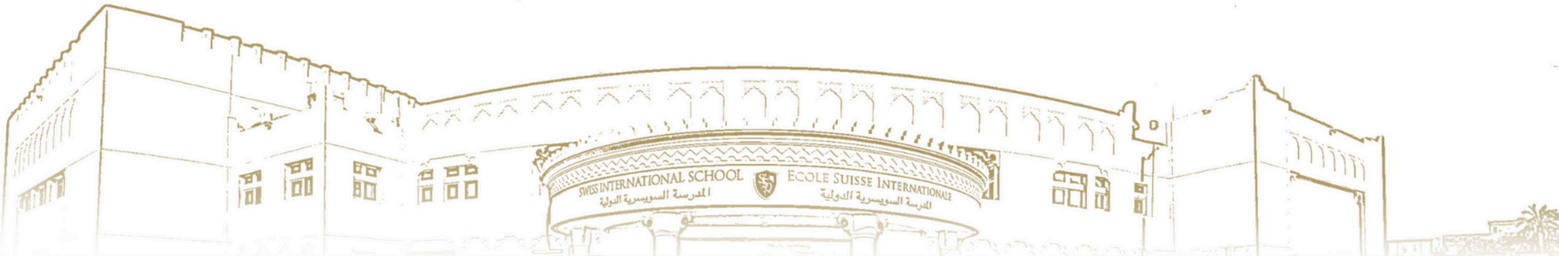
تهدف المدرسة السويسرية إلى تطوير متعلمين يتصفون بأنهم

مُستَعِدون مُلهَمون مُشبَعون

Notre Vision

SISQ encourage les apprenants à devenir

ACCOMPLIS INSPIRÉS PRÊTS


SWISS INTERNATIONAL SCHOOL
المدرسة السويسرية الدولية
ECOLE SUISSE INTERNATIONALE
المدرسة السويسرية الدولية

Our Mission

Through learning that is fun, engaging, holistic, collaborative and caring, SISQ develops students who are:

- Intellectually fulfilled: they find joy in their own learning and the learning of others; they are curious, engaged and passionate about learning.
- Emotionally fulfilled: they are happy with themselves, healthy, balanced and confident.
- Socially fulfilled: they develop meaningful relationships; they are connected to others, the world around them and the environment.

Through learning that is inquiry-based, meaningful, challenging, authentic and innovative, SISQ develops students who are:

- Inspired to keep learning: they are inquisitive, questioning and willing to try new things; they take ownership of their learning and are self-motivated.
- Inspired to share and apply their learning: they can use their learning to improve their lives and the lives of others; they communicate their learning to inspire others.

Through learning that is focused on transferable skills, character, attitudes and dispositions, SISQ develops students who are:

- Prepared for the future: they embrace change and challenge; they adapt to new situations and think creatively to solve complex problems.
- Prepared to lead lives of integrity: they are principled and strong; they have a set of values that guide them when they make decisions.
- Prepared to be good global citizens: they are multilingual, open-minded and multicultural in their outlook; they are courageous, caring and prepared to take action to make their community and the world a better place.

رسالتنا

من خلال المتعة والمشاركة ، والتعاون ، والشمولية والاهتمام ، تعمل المدرسة السويسرية على تطوير طلاب يتصفون بأنهم

- مشبَعون فكرياً، يجدون الفرح في تعلمهم وتعلم الآخرين ؛ إنهم فضوليون ومشاركون ومتحمسون للتعلم.
- مشبعون عاطفياً إنهم سعداء بأنفسهم ، يتمتعون بصحة جيدة ، ومتوازنون ، وواثقون من أنفسهم.
- مشبعون اجتماعيًا: يطورون علاقات ذات مغزى ؛ إنهم مرتبطون بالآخرين وبالعالم من حولهم وبالبيئة.

من خلال التعلم الهادف و القائم على الاستقصاء ، والتحدي والابتكار، تعمل المدرسة السويسرية على تطويرطلاب يتصفون بأنهم

- مُلهَمون لمواصلة التعلم؛ فهم فضوليون ومتسائلون ومستعدون لتجربة أشياء جديدة ؛ يتعلمون بدوافع ذاتية .
- مُلهَمون لمشاركة ما تعلموه وتطبيقه، يمكنهم استخدام ما تعلموه لتحسين حياتهم وحياة الآخرين ؛ ينقلون تعلمهم لإلهام الآخرين.

من خلال التعلم الذي يركز على المهارات القابلة للنقل والمهارات الشخصية والمواقف والتصرفات تعمل المدرسة السويسرية على تطويرطلاب يتصفون بأنهم

- مستعدون للمستقبل يتبنون التغيير والتحدي ؛ يتكيفون مع المواقف الجديدة ويفكرون بشكل خلاق لحل المشكلات المعقدة.
- مستعدون لعيش حياة تتسم بالنزاهة: أصحاب مبادىء أقوياء ؛ لديهم مجموعة من القيم التي توجههم عند اتخاذ القرارات.
- مستعدون ليكونوا مواطنين عالميين صالحين: فهم متعددو اللغات ومنفتحون ومتعددو الثقافات في نظرتهم ؛ إنهم شجعان ومهتمون ومستعدون لاتخاذ إجراءات لجعل مجتمعهم والعالم مكانًا أفضل.

Notre Mission

Au travers d'expériences d'apprentissage amusantes, interéssantes, holistiques, collaboratives, positives, SISQ encourage les apprenants à devenir:

- Intellectuellement accomplis: ils prennent plaisir à apprendre individuellement et collectivement. Ils sont curieux, intéressés et passionnés par leur apprentissage.
- Émotionnellement aptes: ils savent s'apprécier, ils sont positifs, équilibrés et sûrs d'eux-mêmes.
- Socialement compétents: ils développent des relations significatives avec les autres, ils vivent en harmonie avec les autres, le monde et l’environnement.

Au travers d’un apprentissage centré sur la recherche, significatif, comportant des défis, authentique et innovant, SISQ encourage les apprenants à devenir:

- Toujours prêts à apprendre : ils sont curieux, ils posent des questions et sont prêts à innover, ils sont responsables de leur apprentissage et intrinsèquement motivés.
- Toujours prêts à partager et à appliquer leurs connaissances : capables d’utiliser leurs compétences pour transformer positivement leur existence et celle des autres, ils transfèrent leurs apprentissages pour inspirer autrui.

Grâce à un apprentissage orienté vers des compétences de transfert, l'édification du caractère, créant des attitudes et une disposition psychologique bénéfiques, SISQ encourage les étudiants à devenir:

- Prêts pour l’avenir : ils acceptent le changement et les défis, s’adaptent à de nouvelles situations et résolvent des questions complexes grâce à leur créativité.
- Déterminés à vivre de manière éthique, ils suivent leurs principes et sont intègres. Leur valeurs les guident dans la prise de décisions.
- En tant que citoyens du monde: ils parlent plusieurs langues, pratiquent l’ouverture d’esprit en se confrontant à de multiples perspectives. Ils sont courageux, attentionnés et prêts à l’action pour transformer positivement leur communauté et le monde.

1. Policy Statement

1.1. Swiss International School (henceforward referred to in this policy as SISQ), recognises the value of technology in supporting and enhancing teaching and learning and in facilitating school processes and systems. SISQ provides and maintains technology to support the educational programmes and operations of the organisation. This policy describes and defines acceptable and appropriate use of technology, which includes but is not limited to, computer and information systems, networks, peripheral devices, telephone and fax equipment and other technology resources.

1.2. This policy applies to all technology owned or maintained by SISQ, and to all users of, or connected to, this technology, whether on or off campus.

1.3. This policy and its appendices also set out guidelines for the use of social media for SISQ students and employees, with the intention to provide a framework for those interested in establishing a social media platform on which to promote or celebrate SISQ activities. In providing this framework, SISQ is mindful of the responsibility all organisations have to safeguard their own reputations and the wellbeing of their community members within social media, and online in general.

1.4. In addition, this policy sets out acceptable and appropriate use of social media platforms where use of those platforms is either facilitated by SISQ or is associated with SISQ because of the use of SISQ' name, logo or images identified with the school's campuses, personnel or products/services.

1.5. Anyone using SISQ technology does so at their own risk. SISQ is not responsible for any equipment damage or data corruption that may be suffered by the use of SISQ technology.

1.6. As a condition of using SISQ technology, all users agree to comply with this policy as well as with other applicable laws, rules, policies and regulations. Access to SISQ technology is a privilege which the organisation can suspend or revoke at any time.

1.7. All members of the SISQ community are bound by the national laws relating to civil rights, harassment, copyright, data protection, security and other statutes relating to electronic media relevant to their location. This policy does not preclude enforcement under the laws and regulations of the relevant national authorities.

1.8. All members of the SISQ community are expected to conduct themselves with regard to the responsibilities consistent with this policy and all other applicable SISQ policies. Abuse of computing and/or network privileges may lead to disciplinary action, which may include summary dismissal.

1.9. Abuse of networks or computers at other sites through the use of SISQ resources will be treated as though it occurred at SISQ. When appropriate, restrictive actions will be taken by systems or network administrators pending further disciplinary or legal action which may include prevention of further use of SISQ technology, blocking various access, removal of equipment or other security measures.

1.10. This policy is not intended to address each and every situation in which a safe practice matter that involves the use of online technology occurs. In the course of school activities, it is normal for school administrators and other community members to expect all users of technology and online platforms to observe the SISQ values and to respect others. Anyone using online services in a way that compromises the safety, security, wellbeing or respect of others may be deemed in breach of the guidelines contained in this policy, which is offered for the benefit of all SISQ community members and reviewed annually.

2. Policy Guidelines

2.1. The SISQ community is encouraged to make innovative and creative use of technology in support of education, research, academic development and internal administration purposes only. Commercial uses are specifically excluded.

2.2. All students and employees are responsible for ensuring that computer and communication facilities are used in an effective, efficient, ethical and lawful manner and in consideration of others. This policy is intended to respect the rights and obligations of academic freedom.

2.3. In this policy SISQ acknowledges its duty of care over students and commits to following the international best practices in where child safeguarding in concerned.

2.4. We are committed to our vision: SISQ aims to develop learners who are fulfilled, inspired and prepared. SISQ's expected schoolwide learning results extend to all community members and are embodied in the aims of this policy. SISQ expects and believes effective learners, confident individuals and caring contributors to act with integrity and respect with regard to their use of technology. This policy is, therefore, to be viewed as extending from the SISQ values.

2.5. SISQ's guidelines on appropriate use of electronic and digital resources follow three basic principles:

> 2.5.1.Respect for myself – This includes but is not limited to use SISQ's computer network and global telecommunications with honesty and integrity. Keep standards of decency in accessing, viewing, or sending messages and pictures. Keep my password secure. Support copyright laws. Protect and limit the content and accessibility of online information about myself.
>
> 2.5.2.Respect for others – This includes but is not limited to respect others' work and files, their privacy, and their right to access the network. Respect hardware, software, peripherals, and resources that we all share. Respect others' right to feel safe online and in the SISQ community. Be sensitive to the cultural diversity at SISQ.
>
> 2.5.3.Respect for the network management – This includes but is not limited to treat all network management with courtesy and respect. Respect their need to oversee the running of the network. Respect the equipment so that technician time is not spent on machine repair. Get approval for any installation or configuration of software on SISQ computers.

2.6. SISQ provides widespread access for students to technology such as computers and applications, the Internet, and the internal network with the express purpose to support learning.

3. Definitions

3.1. SISQ Technology - The organisation's telecommunications systems including but not limited to telephone, mobile phone, audio visual equipment, lines, transmitters and receivers and data communications and processing systems (including wired and wireless devices, computers, workstations, laptops, iPads, PDAs, printers, servers, scanners, digital still and video cameras and other computer hardware and equipment, software, licensing arrangements, data files and internal computer and communications networks) that can be accessed directly from SISQ computer networks.

3.2. Ownership and Access - In this policy, the terms ownership and access relate to use of computers and technologies that are the property of SISQ and that are made available to user groups including: students (in support of their academic and student life objectives and requirements); employees (in support of their teaching, administrative functions or their assigned responsibilities); and other authorised users (in support of the authorised use of SISQ technology).

3.3. Portable Devices - Laptop computers, iPads and similar devices that are designed to be lightweight and easy to transport. The fast-moving nature of this field of technology means that not all categories of portable devices can be named and identified, but reference to portable devices in this policy should be regarded as covering any device that is not intended to be used in a single fixed location.

3.4 Users - All members of the SISQ community including students, parents, employees, independent contractors, consultants, volunteers, temporary workers, visiting scholars and campus visitors.

3.5. IT Department - Members of SISQ staff involved in deploying, maintaining and developing the school's technology infrastructure. This includes, but is not limited to, the Operations and Finance Manager and the IT Officers. Whenever the decisions actively influence other areas then they will be taken collaboratively with other members of staff (e.g., curriculum related (curriculum itself and methodology of learning the PYP IT Integration Coordinator and the Division Principals, safeguarding the Safeguarding Lead, data protection with the School Life Officer and the HR Manager). If a strategic decision needs to be reached then other members of staff will be called to share their views and ultimately the final decision will be taken by the Head of School and the Board of Directors.

4. Safe Usage

4.1. Access to computers and computer/server rooms must be limited to students and employees who require access for the normal performance of their educational programme/job. Levels of access will be decided by IT department working in cooperation with the Principals of each division and Operations and Finance Manager. All losses and/or suspected compromises to device security should be reported to IT department.

4.2. Computers holding special category data (as defined under the GDPR), and mobile computers should be secured in a locked room or facility during non-school/working hours. Computer system security is the responsibility of all SISQ staff and students, and is overseen by the IT department. Any suspected data security lapses on any system should be reported to IT department and the Operations and Finance Manager.

4.3. All stakeholders should read and familiarise themselves with this Policy. Occasional updates to the policy may be sent to the community via notices publicised at appropriate intervals.

4.4. Academic staff are responsible for ensuring that students understand what constitutes acceptable use of technology (including social media) and that age-appropriate explanations that students can understand and remember are given in lessons, on posters and other printed materials and in other forms determined at the LT level.

4.5. SISQ publishes a separate Password policy. Passwords are for personal use and should be kept secure. Students and employees must not give out their passwords to other students/employees of SISQ, or to any person outside the organisation without appropriate authorisation.

4.6. SISQ recognises that staff members and students may sometimes find external software helpful in teaching or in facilitating their work. However, the introduction of some software without appropriate care and understanding of what functions the software enables may compromise the safe use of SISQ technology for other users, and increases the risk of introducing malware to SISQ' systems and the risk of breaches of data privacy. Staff members and students who wish to use external software, including mobile apps, beta programs and downloads, must obtain prior approval from their appropriate Division Principal/Operations and Finance Manager and final approval from the IT department. In most cases prior approval will be from the Head of School.

4.7. The IT department may authorise teachers to download apps according to the teacher's professional judgement, and where the IT department is satisfied that there is no compromise to data privacy or online safety measures. Where there is any doubt about the potential of software to compromise SISQ' systems, security or other users, a referral should be made to the Head of School by e-mail.

4.8. Misuse of Information Technology, computers, mobile devices and related equipment is a serious disciplinary offence and could lead to action being taken, up to and including dismissal from the organisation. The following is a non-exhaustive list of examples of misuse:
4.8.1. Fraud and theft
4.8.2. System sabotage/introduction of viruses
4.8.3. Using unauthorised software
4.8.4. Obtaining unauthorised access
4.8.5. Breaches of Data Protection laws
4.8.6. Sending or forwarding any message via electronic mail that could constitute bullying or harassment or that could damage the reputation of SISQ.

5. E-mail

5.1. All SISQ staff and students receive SISQ e-mail addresses which are to be used for school-related business. SISQ' e-mail system can be monitored after approval of the Operations and Finance Manager in case of misused suspicion. In the event of a safeguarding concern related to a school account, the Online Safeguarding Lead, acting on behalf of the school safeguarding team, may access any relevant account as part of the safeguarding investigation process.

5.2. SISQ is mindful that e-mail is known to be one way those wishing to do harm to children have made their initial contact and begun the process of grooming. SISQ staff are, therefore, reminded of the need to be vigilant for signs of the potential misuse of e-mail.

5.3. SISQ e-mail accounts are provided under the assumption that they will be used for work-related purposes. In particular, users are reminded that their access to their SISQ e-mail account and its contents will cease when they leave SISQ and the account is closed, but that SISQ may be required by authorities such as the data protection regulators to reopen and access closed accounts, and disclose any information that might be relevant to a subject access request or similar investigation. Users' attention is drawn to the contract of employment which outlines the terms of use of this account.

6. School Website and Internet Access

6.1. SISQ provides staff, students, community members and visitors to the campus with online access free of charge. Access to the Internet and to online resources on SISQ campuses is subject to filtering and monitoring procedures that are reviewed regularly.

6.2. SISQ will not tolerate the use of online access for illegal activities or for activities inappropriate to a school setting intended to be a safe place for learning.

6.3. Under no circumstances should SISQ network security be circumvented using tools such as VPNs (virtual private networks), proxies or any other method of 'traffic tunnelling' designed to masquerade activity or locality unless specific authorisation is obtained from the IT department.

6.4. Displaying or downloading information or images that are offensive, obscene, abusive, objectionable or dangerous is not permitted. Sensitivity to the diversity of the SISQ community will be considered in deciding whether or not material is offensive.

6.5. Using another person’s password, or trespassing in another person’s folders, work or files is not permitted.

6.6. Using the SISQ Internet for personal financial gain or personal commercial activity such as offers of products or services, etc., is not permitted.

6.7. All users are expected to abide by the following generally accepted rules of network etiquette:

- Be polite, do not be abrasive in your communication to others.
- Use appropriate language. Do not swear or use vulgarities or other inappropriate language.
- Note that the SISQ Intranet is not a place where privacy can be guaranteed.
- Respect the intellectual property of other users and information providers.
- Respect the privacy of others with regard to use of images, video and other content..

7. Information Systems

7.1. In order to maintain the confidentiality of information on SISQ’ computer information systems, SISQ employees and students are required to abide by all security measures established by SISQ to safeguard information systems. These include, but are not restricted to: passwords, access safeguards and identification processes.

7.2. SISQ employees and students are required to ensure they have appropriately secured their device’s privacy when leaving them unattended. For example, by logging out of the SISQ network or locking their device via a secure password.

8. Portable Devices

8.1. SISQ employees and students who have been allocated a portable device are regarded as the device’s owners for the duration of their employment or matriculation at SISQ, and are required to take reasonable care of their portable device at all times. Reasonable precautions must be taken to keep the device secure and to safeguard the information stored on it. Portable device owners are expected to be especially mindful of the danger of theft in public locations.

8.2. SISQ employees and students are referred to the terms and conditions attached to the SISQ portable device scheme and are reminded that SISQ may, at its discretion, require employees or students to meet the costs of any repairs or replacement against loss or damage that may arise from carelessness with their portable device.

8.3. A SISQ employee or student who is allocated a portable device is the person authorised to use that device and the software on it. They may not distribute user rights to another party. Data stored on the portable device must be backed up regularly as protection against theft or mechanical malfunctions.

9. Cloud-based Collaborative Tools and Shared Drives

9.1. SISQ recognises and acknowledges the ubiquity of cloud-based tools such as Google Drive so forth that are designed to facilitate collaborative work. SISQ regards it as a professional expectation that contributors to documents shared via such services ensure the content they add is accurate and that it constitutes fair processing. Among other things, this means acting to rectify any false information as soon as it is recognised as false.

9.2. When using such tools for school purposes, SISQ expects users and contributors to use professional judgement, and to abide by the relevant data protection legislation and SISQ’ own Privacy Notice (see Data Protection Policy).

9.3. In particular, SISQ as a data controller expects its staff to recognise and abide by their responsibility to protect and uphold the rights of data. Among other things, this means taking appropriate steps to ensure data shared via such collaborative tools is not shared with unauthorised persons, that editing privileges are not abused or extended to those for whom read-only access is more appropriate, and that all data processing via such tools is done in accordance with the principles of fair processing.

10. Distance Learning Tools

10.1. Like other schools, SISQ employs various distance learning tools to ensure continuity of teaching, learning and essential business during times when the school may be closed owing to exceptional circumstances such as extreme weather or a pandemic. This policy is deemed to cover these circumstances and normal site-based activities equally.

10.2 Students who engage in distance learning are required to indicate their understanding that lessons conducted online synchronously (i.e. live, at the time the lesson is taught by the teacher) may be recorded for the use of students learning asynchronously (i.e. later, after the lesson has finished), as well as for the monitoring and improvement of quality. The usual data privacy rights apply to such lessons, including data retention periods.

10.3 Faculty who are teaching in a distance learning forum are deemed to be working under the SISQ Code of Conduct and all relevant policies regardless of their physical location at the time the lesson is taught.

10.4 In addition, faculty must abide by the relevant online policies in use at SISQ when teaching distance learning lessons. In particular, faculty’s attention is drawn to the dress code associated with such lessons, the suitability of the location from which the lesson is taught and the safeguarding precautions required to be followed.

10.5 Distance learning lessons that involve one-to-one student-teacher arrangements must be appropriately risk assessed and signed off by the relevant divisional administrator (principal or assistant principal)

10.6 During periods of school closure, SISQ recognises that private tutoring arrangements that are normally permitted to take place on school premises for the convenience of students and their families, will in many cases continue on a distance learning basis. During such periods, communication between tutors and students must not be facilitated using SISQ devices. Instead, tutors must use privately owned devices and e-mail accounts when they undertake private tutoring.

10.7 All considerations regarding behaviour and respect apply equally to online/distance teaching and learning and site-based teaching and learning.

11. Mobile phones and the SISQ Telephone System

11.1. SISQ monitors its telephone system on a regular basis. SISQ employees are advised that SISQ reserves the right to monitor the destination and length of outgoing calls where it has grounds to suspect serious or constant misuse of its telephone system.

11.2. SISQ employees who are issued with mobile phones for use at work must ensure the security of the phone (and any allied equipment) at all times.

11.3. SISQ employees are expected to use mobile phones that are issued to them responsibly and to declare and reimburse costs incurred for any calls made for personal purposes not connected with SISQ business.

11.4. When agreed beforehand and approved by the Operations and Finance Manager, employees who use their personal mobile for business purposes may be reimbursed for business calls.

11.5. SISQ employees are expected to remain up to date and informed about national laws regarding the use of mobile phones.

12. Prohibited Activities

12.1. SISQ recognises the formal definition of malicious communication as sending a letter or electronic communication with intent to cause distress or anxiety.

12.2. Users shall not use SISQ technology, directly or indirectly for illegal or inappropriate activities. Such activities include, but are not limited to:
Creating, facilitating, or performing any illegal activity or violating the legal rights of others.
Circumventing the user authentication or security of any device, host, network, application, or account (including hacking, breaking in, or stealing files or data) or using, disclosing, or changing another person's password, without the express consent of that person or the appropriate person in authority at SISQ.

Posting, transmitting, communicating, or disseminating content which violates the rights of others or which is unlawful, malicious, threatening, abusive, libellous, slanderous, harassing, defamatory, offensive or objectionable to a reasonable person.

Uploading, downloading, posting, publishing, transmitting, retaining, reproducing, sharing, or distributing in any way information, software, movies, music, books, articles, or any other material which is protected by copyright or other proprietary right(s), without obtaining permission of the owner.
Using any SISQ-owned computer to access, post, transmit, or disseminate obscene or pornographic content.
Copying, modifying, utilising, or sharing software in violation of a software lisence.
Restricting, inhibiting, or otherwise interfering with the ability of others to use or enjoy SISQ technology, including generating levels of traffic sufficient to impede others' ability to send or retrieve information or wasting technology resources. This includes printing too many copies of a document or other unnecessary output; using networked resources for recreational purposes; and high-bandwidth activities such as uploading, downloading, or sharing software, music, video, and other media files whether through FTP, a centralised service, through peer-to-peer sharing or other arrangement for personal or recreational use.
Diverting or intercepting network transmissions unless authorised to do so.
Engaging in fraud, misrepresentation, "phishing," or falsifying addressing information to conceal, spoof, or mask a sender or recipient's identity.
Using SISQ technology for commercial purposes (other than SISQ business) or unauthorised financial gain.
Violating the policies of, or disrupting activities on computers and mobile devices used in school.
Misusing, tampering with, altering, stealing, vandalising, defacing, or intentionally damaging any SISQ technology.
Disseminating "SPAM" (unsolicited commercial and non- commercial e-mail) or initiating or participating in the promulgation of chain letters, unauthorised automated or mass postings, or other types of unauthorised large-scale distributions.
Invading the privacy of, or inappropriately distributing the phone number(s), e-mail addresses, or other personal information of, another person.
Posting confidential information on the Internet about SISQ, its customers, suppliers, employees or students, any other as foreseen in the Qatari Laws

13. Privacy

13.1. SISQ commits to respecting all privacy rights in keeping with its observance of the SISQ Privacy Notice, SISQ Data Protection Policy and Qatar Law No. 13 of 2016.

13.2. Within the bounds of this policy, the Data Protection Policy, the Safeguarding Policy and in accordance with all applicable laws, SISQ may monitor the activities and communications of its users. For example, SISQ may monitor the activities of students and employees when needed to investigate a possible disciplinary offence or violation of law or the SISQ codes of conduct, or to help ensure the proper operation of SISQ technology. All users agree to such monitoring through their use of SISQ technology. If monitoring shows possible evidence of improper or illegal activity, such evidence may be turned over to SISQ authorities and/or law enforcement officials.

13.3. Forensic online monitoring is carried out daily and weekly to enable SISQ to appropriately safeguard students and ensure that all staff online use is compliant with the Code of Conduct.

13.4. Staff who appear in the forensic online monitoring log will be recorded in the first instance if the monitoring log indicates inappropriate content. The data will be reviewed and the member(s) of staff concerned will be alerted to the occurrence.

13.5. Staff who appear in the forensic online monitoring log repeatedly for inappropriate content or appear in the log due to illegal or potentially harmful content will be referred to the Head of School and/or HR department and if necessary, the appropriate outside agency such as the safeguarding authorities or police.

Appendix 1: SISQ Expectations - Student Usage of IT Resources and Behaviour

General Expectations

- With the privilege of access comes the expectation of responsible use. Responsible use includes:
  - Treating the equipment well.
  - Keeping the network and school computers free of viruses, spyware, and/or adware.
  - Using the resources in a manner that does not harm self or others.
- These are non-negotiable expectations, and deliberate violations of these expectations will lead to disciplinary consequences

On Campus Computers Use

- Users who damage IT equipment may be charged for the repairs.
- All non-SISQ electronic devices (bring your own device) such as laptops must be registered with the IT department in order to get access to the school network.
- This helps protect the school network from viruses and unauthorized access. Misuse of the system by a user can result in this registration being revoked

Off Campus Computers Use

- In such instances that students require access to school devices off campus, the school may provide a limited number of devices for home use. Users who damage a device may be charged for repairs and the same rule governing the use of a device on campus will apply off campus. We expect all SISQ community members to adhere to the same ethical conduct at home as they do at school.

executable files onto the

Use of School Accounts

- To facilitate the use of devices in the classroom and during online learning, students may be given access to online services provided by the school. These may include, but are not limited to, Google, Renaissance, Toddle, MyOn, etc. Students commit to using these accounts exclusively for educational purposes in connection with the tasks or activities assigned by their teachers. Misuse of school accounts may result in the temporary suspension of the relevant account. Continued misuse may result in the account being blocked.

Device Use at Home

- In the event that a student is required to use a device to learn from home, parents and guardians agree to take the necessary steps to keep their children safe online. This may include installing anti-virus software on devices, ensuring filters are used to prevent access to inappropriate content and monitoring internet usage. Parents and guardians agree to report any incident of misuse which they believe could affect others directly to the school.

Privacy and Passwords

- Students may be provided with personal network space in which to save their work. This space is treated by SISQ administration like a physical school locker. It is respected as belonging to an individual but it is open to inspection by SISQ administrators should there be due cause (e.g. virus, inappropriate content, exceeding storage limits, etc.).
- Students should never use someone else's password and/or access their account without permission. Any attempts to "hack" into accounts or determine others' passwords will be treated as a dishonest act of vandalism and as a violation of our code of ethics.

Virus Protection

- Students may not boot SISQ computers with their own disks, nor copy system or executable files onto the computers.
- Additionally, we strongly recommend and request that students' home computers be kept up to date in anti-virus protection. Viruses from home are quickly transferred to school through USB drives and corrupted files. It is the users' responsibility to ensure that their USB drives do not bring harmful files into the school network.

Software

- SISQ is committed to the legal use of software. We support international copyright laws. Users should never download or install any commercial software, shareware, or freeware onto network drives or disks, unless they have network administrator permission.

Inappropriate Content, Language or Use

- No profane, abusive or impolite language should be communicated using SISQ electronic resources. Content should not be accessed which is not in line with rules of school behavior. A good rule to follow is never access, view, or send materials which you do not want all teachers or parents to view while sitting next to you. Should students encounter such material by accident, they should report it to their teacher immediately.
- If a website or online activity becomes a distraction from learning, this site or activity will be blocked by SISQ network administration.
- Repeated access to an inappropriate site will be referred to the Division Principal.
- In line with the school's commitment to keeping children safe, if there is suspicion of device misuse, any device brought to school may be confiscated and inspected as part of an investigation. This applies to both personal devices and those provided by the school.

Social Networking

- Online safety is a personal responsibility. It is important that students are aware of the implications of their actions online, both on themselves and on others. The actions students take on social networking sites like Facebook or Twitter can impact their university applications, job searches, and overall reputation. It can also provide sensitive information to online predators.
- Students should keep themselves and the people they know safe by carefully screening who their online "friends" are and what information they share as well as locking down privacy settings.

Cyber-Bullying

- No form of bullying is tolerated at SISQ, cyber-bullying included.
- SISQ becomes involved when a student's online activities impact at-school life and community.
- If the actions of students outside of school have an effect on students feeling unsafe or uncomfortable at school, then SISQ administration will act and remedy this. Additionally, if members of SISQ staff or its community are targeted, then the school administration will get involved.

Photo and Image Usage

- SISQ employees and associates may take or use photographs or other media that include student images, exemplars of student work and/or images of students taking part in a school events or activities. Parents and guardians will be provided with the opportunity to opt out of providing consent for this at the start of each school year or when a new student is enrolled.
- These photographs/media are used to provide SISQ families with information about their child(ren)'s education and/or to provide information to other parties about SISQ. The images must be taken on school owned devices and may be published on SISQ approved platforms.
- Parents may opt out of having the school use images or work of their children for SISQ promotional materials. If there are questions or concerns, parents should arrange to meet with the relevant Division Principal.

Academic Malpractice

- Students agree not to participate in academic malpractice (also known as academic dishonesty) in any form. This includes the use of electronic devices to engage in plagiarism or to gain academic advantage. Academic malpractice includes, but is not limited to:

  - Collusion: supporting malpractice committed by another student, such as by allowing them to copy work or submitting work done by another student as one's own. It also includes working with others on supposedly individual assignments, or allowing another person (student, parent or tutor) to revise, edit or write work which is then submitted as the student's own.
  - Duplication: re-submitting a piece of work for more than one assessment.
  - Fabricating data: making up results for experiments or creating false citations.
  - Falsifying student records: for example, adjusting grades or teachers' comments.
  - Plagiarism: representing ideas or the work of others as one's own. It may involve copying another student's work, failing to correctly acknowledge (cite) the sources used or including in-text citations that do not match the Works Cited page.
  - Unfair advantage: any behaviour that gains, or attempts to gain an unfair advantage for one student or affects the work of other students, such as accessing unauthorized materials during an examination, disruptive behavior in examinations, damaging work of other students, stealing examination/test papers or downloading them from the internet.

- As appropriate, student work will be reviewed using TurnitIn to check for authenticity and plagiarism. All instances of academic malpractice will be investigated and reported to the relevant section principal and appropriate courses of action will be implemented to rectify student behaviour and attitude in line with the school's academic honesty policy.

Appendix 2: Social Media, Blogging, Social Networking and Messaging

- SISQ recognises the legitimate useful purposes a blog or a social networking or messaging platform may serve to showcase class activities, support students' learning, display student work, facilitate telecollaborative projects and so forth. Blogs from outside providers may be linked to teacher pages provided the authors of such blogs are mindful of their responsibilities under the Data Protection Law of Qatar, national laws including copyright laws, and any statement by an SISQ community member regarding the use of their personal image or, in the case of an SISQ parent, the image of their child.
- SISQ acknowledges the ubiquity of social media and its potential to support and enhance learning. SISQ also recognises that use of social media can be a distracting element in school learning activities. Division Principals, Manager and the Head of School are expected to establish guidelines for respectively teachers and support staff on the appropriate use of social media during working hours. The terms and conditions associated with each social media platform will normally constitute the first consideration with regard to its appropriateness for use in a given learning setting with children.
- SISQ recognises the growing importance and benefits of communicating through social media. As SISQ' own activity on social media has grown – and as the social media activity of SISQ' community members has grown, so a greater understanding and appreciation of the potential benefits of social media has developed. SISQ recognises that students and staff may be interested in promoting their work to the online community through social media, and thereby becoming advocates for SISQ.
- SISQ recognises that social media is a fast-changing category of online activity and that various social media platforms have risen to prominence in recent years, some of which have endured and some of which have faded to obscurity.
- SISQ recognises certain identifying characteristics of social media such as its user- generated aspect and the fact that its content is generally shared online.
- SISQ has established a number of official SISQ social media channels on popular social media platforms including Facebook, Instagram, Twitter, YouTube and Linked In. In addition, other social media tools in use across the organisation include blogs, micro blogs, wikis, chat rooms, online communities, and video platforms (such as Vimeo).
- SISQ takes social media responsibility seriously. All SISQ social media accounts are considered official communication channels. It is a requirement that any SISQ accounts (accounts that use SISQ in the title and speak on behalf of SISQ) are set up with the Marketing Department and run to profession standards, and that SISQ is aware of who is representing the organisation via the social media. For this reason, any staff member ishing to become official account holders of social media platforms representing SISQ are advised to contact the Marketing Department.
- SISQ advises all staff members who become official SISQ account owners that they will be fully responsible for the management and content of the account. Social media accounts need regular monitoring and checking daily, including weekends, and out of hours by account owners to ensure that messages and posts can be responded to in a prompt and timely manner. SISQ keeps a record of official accounts and spokespeople and monitors activity. Any social media accounts using SISQ will be picked up through monitoring tools.

- SISQ students are personally responsible for the content that they post, share and respond to online. When posting online, all information is considered representative of the poster's views and opinions and may not be assumed to represent the views of SISQ.
- SISQ strongly advises users to recognise that online postings and conversations are not private. SISQ community members are warned of the potential consequences of sharing confidential information, internal school discussions or specific information about students, staff or other community members via social media.
- Users of social media may not refer to SISQ in the names of social media accounts, or use SISQ logos or images that are associated with SISQ unless the account is an official account approved by SISQ.
- SISQ staff members are reminded of the inadvisability of friending students on social media. Staff are referred to the Online Safety Policy and to the SISQ Staff Handbook and Code of Conduct for further information. Staff are further reminded to respect the privacy of other staff members and other community members and their preferences regarding their social networks.
- All SISQ community members are reminded that the school's values are expected to guide all behaviour whether on or offline. Students are expected to follow all SISQ policies when online, and to conduct themselves as if at school. SISQ will work in partnership with parents to monitor behaviour that negatively affects our students or reflects poorly on the values of the organisation, and students may face consequences for behaviour that violates SISQ' values and policies.
- When posting, even on the strictest settings, community members should act on the assumption that all postings are in the public domain. Community members are reminded that in microblogging (Twitter etc.), comments made using such media are not protected by privacy settings.
- SISQ' users of social media are reminded that under no circumstances should offensive comments be made about students, parents, staff or SISQ in general. If responding to someone with whom they disagree, SISQ stakeholders are reminded of the importance of respectful language and of the need to ensure any criticism offered is constructive and not hurtful. Posts and comments should help, build and support the SISQ community.
- In the same vein, SISQ community members are reminded not to comment on or forward unsupported information such as rumours and to ensure that their profile and related content is consistent with how they wish to present themselves to colleagues, parents, and students.
- SISQ acknowledges that pictures and other content posted on social media are public and information can be shared beyond the control of the original poster. Students are taught to consider whether posted content would give an unfavourable impression of the poster to potential future viewers including friends, parents, teachers or future employers, or provide damaging material to persons ill-disposed towards the poster. Students are taught that although it is often technically possible to remove content from the Internet or make it hard to locate, it can often be extremely difficult to undo the damage that ill-advised posts hold the potential to cause.
- SISQ has a separate Password policy that is intended to provide guidance to community users on safeguarding access to their online presence in all forums including social media. SISQ expects users of online forums to observe this policy. Users are required to keep passwords.
- ·SISQ students are further advised not to give out personal information, (including, but not limited to, last names, phone numbers, addresses or exact birthdates) on social media, and to accept social network invitations only from people they know.

- SISQ publishes a separate Child Protection and Safeguarding policy that describes the support available to children and other community users if they feel unsafe online.
- In addition, SISQ publishes a separate Online Safeguarding Policy. Students who find themselves in a social media interaction where they feel threatened or unsafe are encouraged to tell a parent or trusted adult immediately and to report any difficulties or escalating situations that are associated with school-sanctioned use of social media to a teacher or Principal.
- SISQ staff who are using a social media account that identifies them as a member of SISQ are reminded of the professional expectations contingent upon them. The guidelines in Appendix Two of this policy are set out as advised good practice and should not be regarded as comprehensive. Social media is a fast-changing field of human activity and staff are expected to employ common sense and professional judgement in all their decisions regarding what they post on social media platforms, whether or not SISQ is the subject of the post.

Appendix 3: Best Practice Guidance on Use of Social Media

Identification of Poster

- Staff may mention that they work for SISQ and may discuss SISQ and promote their work. However, they must make it clear that views expressed are personal and not those of SISQ.
- Staff should refrain from making reference to SISQ, its employees, customer and suppliers on social media. Their name or social media handle/title should not contain SISQ in any form. Only approved SISQ accounts with approved SISQ spokespeople are authorised to do this.
- Staff should be alert to the beguiling nature of the informality associated with many social media platforms. They should exercise care in what they say and be alive to the possibility that what they post may quickly be shared to other parties outside the control of the original poster or governing legislation.

Integrity

- Staff are expected to be transparent and state that they work for SISQ. Their honesty will be noted in the social media environment. If staff members are writing about SISQ or about a competitor, they are expected to use their real name, identify that they work for SISQ, and be clear about their role.
- Where staff have a vested interest in what they are discussing, they are expected to be the first to say so.
- Staff are expected to post meaningful, respectful comments and to avoid posting spam or making remarks that are off-topic or offensive.
- Staff are expected to stick to their area of expertise and to feel free to provide unique, individual perspectives on non-confidential activities at SISQ.
- When disagreeing with others' opinions, staff are expected to keep their comments appropriate and polite. If an online situation appears to be becoming antagonistic, staff are expected to handle the situation with professionalism. This may require consulting with a colleague or line manager or it may require disengaging from the discourse in a polite manner that reflects positively on both the staff member and on SISQ.
- Staff are expected to seek appropriate guidance from a line manager before participating in social media when the topic being discussed may be considered sensitive (for example an incident or crisis situation, or a situation involving an intellectual property or commercially sensitive dispute).
- Staff are reminded that a swift an honest apology for any mistakes made in both consistent with professional expectations and provides a foundation for trust for future social media activity.

Defamation and Libel

- On an online social network any comment posted is clearly linked to the poster and their profile. Users of social media need to carefully consider what they post and be mindful of other peoples' views and feelings. In legal terms, content posted on social media is usually covered by laws relating to libel and defamation.
- Content posted on social media constitutes evidence which courts can consider and require to be disclosed for use in litigation. Such content may be used as a reference with regard to interviews or other career decisions. SISQ staff are reminded that in recent years UK libel courts have been used to recover damages for libel against posters of comments, tweets and other content on social media that was ruled to be defamatory.

- Guiding Questions for Users of Social Media when Reviewing Content Prior to Posting
  - Are you happy for this information to be in the public domain?
  - Is the content derogatory, defamatory, discriminatory or offensive in any way, or could it bring SISQ into disrepute?
  - Are you representing yourself or SISQ in a false or misleading way?
  - Are all statements true and not misleading, and can all claims be substantiated?
  - Does the post display common sense and common courtesy? For example, has permission been sought to publish or report on conversations intended to be private or internal within SISQ?
  - Have efforts been made to be transparent and to avoid breaching SISQ' Privacy Notice and/or legal guidelines for external communication?
  - If the content of the post involves SISQ' competitors, is the post appropriately diplomatic, factually correct and accompanied by any necessary and appropriate permissions?
  - Are appropriate privacy protections in place for both the poster and SISQ? Is confidential information involved, and if so how is it safeguarded?

Posting images at SISQ

- In accordance with the Online Safety policy, SISQ staff may not upload pictures to any social media (including photo sharing platforms such as Instagram, Flickr and Pinterest) of clearly identifiable SISQ students or staff members who have not consented (or, in the case of children, have not had their legal guardians consent) to have their images shared in this way. This includes images of single students and images of multiple students that include a student where consent has not been granted.
- Where there is any doubt about which students or staff have consented to permit their image to be shared, (or, where appropriate, have had consent granted on their behalf), the poster must contact the appropriate divisional secretary or other administrator for details of which students do not have image permissions.
- If there is continued uncertainty about permissions following reasonable steps to establish permissions, staff are advised not to use the image in question.
- The photo-tagging tool on Facebook and similar/comparable technologies in any social media platform must always be disabled if using pictures of students.

Publicising events at SISQ

- Staff are required not to publicise school events on social media before they happen. SISQ' policy is to promote events after they have taken place.
- Exceptions include some parent organised events that do not take place on campus, or events which Division Principals or Head of School have agreed may be promoted beforehand.
- In case of doubt, staff are expected not to promote the event, or to check with an appropriate line manager or with the Marketing Department.

Monitoring/Regulation of Social Media

- Staff are expected to understand and recognise that social media is an interactive form of communication. It is expected that users will monitor their accounts and respond as necessary on an ongoing basis. This includes remaining watchful for security breaches.
- Staff are expected to remain educated about risks to social media accounts, and in particular the dangers associated with accounts being compromised by an external attack or hack. Staff are advised to exercise care clicking on unidentified links in social media channels. Staff are also expected to block spammers and users who are abusive or inappropriate.
- Division Principals will offer support at SISQ for any staff member who experiences difficulty or who finds themselves in an escalating situation as a result