Digital Safety Policy

Introduction

The safety and welfare of our students is our highest priority and SISD's digital safety policy reflects the importance on the safe use of information systems and electronic communications. Digital safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles etc. using wired and wireless technology. It highlights the need to educate students and staff about the benefits, risks, and responsibilities of using information technology.

It provides safeguards and awareness for users to enable them to control their online experience. Internet access is planned to enrich and extend learning activities and the school has acknowledged the need to ensure that all students are responsible and safe users of the Internet and other communication technologies.

Scope of the Policy

This policy applies to all members of the school (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. This policy provides clarity about the use of electronic communications in a manner that is safe and deters users from accessing inappropriate information.

SISD has a Digital Safety Coordinator who is a member of the Safeguarding team who support digital safety in the school and ensure that this remains a high priority. Although the school offers a safe online environment through filtered internet access, we recognize the importance of teaching our students about online safety and their responsibilities when using communication technology. In addition to online safety being taught in classes and during internet safety day, staff CPD includes updating their own knowledge on the current risks (and possible solutions). In addition, the school offers information and advice to parents using a variety of means.

The aim of this policy.

- Protect and educate the whole school community from illegal, inappropriate, and harmful content or contact in their use of technology.
- Responsible ICT use by all staff and students.
- Safe and secure internet filtering
- Implementation of this policy in both administration and curriculum, including secure school network design and use.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the Digital Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about digital safety incidents and monitoring reports. A member of the Governing Body has taken on the role of a Digital Safety Governor. The role of the Digital Safety Governor will include:

- Regular meetings with the Digital Safety Coordinator

- Regular monitoring of digital safety incident logs
- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors / Board / Committee / meeting

The Principal and Senior Leaders:

- The Principal and Senior Leaders has a duty of care for ensuring the safety (including online safety) of members of the SISD School community, though the day-to-day responsibility for online safety will be delegated to the Digital Safety coordinator and the Safeguarding Team.
- The Principal, the Designated Safeguarding Lead and the Designated Digital Safety Coordinator will work together and should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a student or a member of staff.
- The principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

Digital Safety Co-coordinator (DSC):

- The Designated Safeguarding lead (DSL) and DSC jointly work on establishing and reviewing the Digital Safety Policies.
- Supports staff and leads the digital safety awareness, issues in consultation with the safeguarding team.
- Joins the safeguarding meetings once every month to discuss updates and concern related to digital safety in Primary and Secondary.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an incident taking place in consultation with the safeguarding team.
- Provides training and advice for staff and technical staff during induction.
- Receive reports of online safety incidents, that are monitored by DSCs and shared in safeguarding meetings to discuss plans and digital safety developments.
- Ensure that the school infrastructure is secure and is not open to misuse and malicious attack with support from the IT department.
- Coordinate with the IT department in filtering websites for students and monitoring usage.

Safeguarding Team:

- The team should be trained in Digital safety issues and be aware of potential serious child protection or safeguarding issues that arise such as sharing of personal data, access to illegal materials, in-appropriate online contact with adults, cyberbullying.
- Support DSCs in the event of an incident taking place related to digital safety.

Network Manager / Technical staff:

The Network Manager and IT department is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required digital safety technical requirements and any KHDA / other relevant body Digital Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with digital safety technical information to effectively carry out their role and to inform and update others as relevant.

- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of Year / Principal / Senior Leader, Digital Safety Coordinator.

Teachers and Support Staff:

- Should act as good role models in their use of digital technologies, the internet, and mobile devices.
- They have an up-to-date awareness of digital safety matters and the school's digital safety policy and practices.
- They report any suspected misuse or problem to the Head of Section for investigation / action (*see Appendix 1*) for the referral procedure.
- All digital communications with students / parents / carers should be on a professional level and only carried out using official school systems.
- Digital safety issues and awareness are embedded in all aspects of the curriculum and other activities such as using video link instead of YouTube.
- Students understand and follow the digital safety and acceptable use policies.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies regarding these 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.

Designated Safeguarding Lead:

Should be trained in digital safety issues and be aware of the potential for serious child protection / safeguarding issues 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:

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy.
- Are provided with an 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 and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras.
- They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good digital safety practice when using technologies out of school and realize that the school's Digital Safety Policy covers their actions out of school, if related to their membership 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 digital safety campaigns / literature. Parents and caregivers will be encouraged to support the school in promoting good 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 / blog
- Their children's personal devices in the school (where this is allowed)

Education and Awareness

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 digital safety is therefore an essential part of the school's digital safety provision. Children and young people need the help and support of the school to recognize and avoid digital safety risks and build their resilience.

- Key digital safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities such safer internet day.
- 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 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, the internet, and mobile devices.
- 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.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Caregivers

Parents play a crucial role in the education of their children and to monitor their online usage. Parents may misjudge how often children and young people could be vulnerable online and come across potentially harmful and inappropriate material on the internet. To support parents, the school will share information regarding Digital Safety

- Letters, newsletters, website
- Events and Awareness sessions
- Resources for relevant sites.

Education & Training – Staff / Volunteers

Training will be offered as follows:

- A digital safety training will be organized every academic year for some staff in key positions who would then share the message within their teams.

- All new staff should receive digital safety policy as part of their induction programme, ensuring that they fully understand the school digital safety policy and Acceptable Use Agreements.
- The Digital Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (e.g., from relevant organizations) and by reviewing guidance documents released by relevant organizations.
- This Digital Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INDUCTION days
- The Digital Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / e-safety / health and safety / child protection. This may be offered in several ways:

- Attendance at training provided by the KHDA / National Governors Association / or other relevant organization.
- Participation in school training / information sessions for staff.

Technical Infrastructure

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 digital safety responsibilities:

- School technical systems will be managed in ways that ensure that the school 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 technical systems and devices.
- The Network Manager is responsible for ensuring that software license logs are accurate and up to date and that regular checks 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 etc. 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.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g., trainee teachers, supply teachers, visitors) onto the school systems
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies to provide a greater freedom of choice and usability.

However, there are several safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments.
Considerations will need to include levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing, and monitoring. This list is not exhaustive, and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement (refer to acceptable use policy)
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's / academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff

Reporting Procedure

Allegation or concern about online safety

- The school treats the safeguarding of the students in its care as the highest priority and recognizes the important role it must play in monitoring and educating students and parents about online safety.

- All staff should recognize that children can abuse their peers via mobile devices or the internet. Different forms of peer-on-peer abuse can take place, but abuse is abuse and should never be tolerated or passed off as "banter" or "part of growing up". This is most likely to include, but not limited to: the problems around sexting and cyber bullying.

- All staff and volunteers should feel able to raise concerns about online safety issues and that such concerns will be taken seriously by the DSC and DSL.

- The school will seek advice from agencies and professionals and act in accordance with both national and local guidance to tackle the concerns appropriately and work in partnership with those agencies.

- The sending of indecent images from one person to another through digital media devices is a safeguarding concern, contact the DSL or your Deputy Head Pastoral. Please refer to procedures of safeguarding in the Child protection and safeguarding policy.

- If there is abuse by one or more students against another student, then reference should be made to the Anti-Bullying Policy. Allegations should be reported to the Deputy Head Pastoral / DSL.

Procedures for dealing with an allegation brought to a member of staff by a student

- If an online safety issue is brought to the attention of a member of staff, they should:
  - listen to the child, to provide re-assurance and to record the child's statements, but not to probe, interrogate or put words into the child's mouth or ask outright whether s/he or others have suffered abuse.
  - limit questioning to the minimum necessary for clarification.
  - avoid leading questions.
  - refrain from giving any inappropriate guarantees of confidentiality; instead, the child should be told that the matter will be referred in confidence to the appropriate people in positions of responsibility.
  - the matter should be taken seriously, and the appropriate staff informed.
  - listen but must not judge and should reassure the pupil that s/he has done the right thing in speaking to an adult.
  - Members of staff must make it quite clear to the student that they cannot offer confidentiality and that they will have to tell others. Only those with a need to know should be informed.
  - Staff should not attempt to carry out an investigation themselves.
  - For pictorial view of a response to an incident of concern – see appendix 1.
  - For specific procedures relating to cyberbullying please refer to Anti-Bullying Policy.

Procedures for dealing with an allegation if concern is raised by the IT department

- A search on a machine would normally be undertaken with the student's consent but not necessarily in the presence of the student. Signing up to the Acceptable Use Policy constitutes consent.
- When searches are made, the search is logged and conducted in the presence of two members of IT staff or DSC. Students will be contacted to provide access details and may request to be present if required. If a device is removed from a study (for example, when causing network disruption), a sheet is left, advising the student to contact the IT Department, and the Housemaster is informed via email. It is also possible for a replacement machine to be left so as not to hinder academic work.
- Consequences – these are proportionate to the content and amount of material found on the electronic advice. Refer to the Pupil Behaviour and Management Policy for offences and sanctions.

Procedures for dealing with an allegation if concern is raised against a member of staff

With respect to any allegation made against a member of staff regarding online safety, the Head of Section and Principal should be informed immediately, and reference should be made to the Safeguarding and Staff Code of Conduct.

Technological Risks

Student Mobiles

- Student mobiles are permitted in school but is prohibited during school hours and should remain in their bags/lockers.
- Mobiles are permitted in Boarding. Grade 9 and below have them in overnight at roll call. Grade 10 and above are permitted to keep them provided they are maintaining expected academic commitment and behaviour levels.
- Mobile phones are permitted in a teaching setting provided permission has been sought and granted by the member of staff in charge of the class.
- Mobile phones should not be used when walking around the school premises.
- Mobile phones may only be used to take photographs of individuals if permission has been sought and granted by the individual concerned and that the Acceptable Use Policy is always applied.
- Special attention should be taken to identify trends in mobile social media/messaging sites.

Use of Digital and Video Images

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognize the risks attached to publishing their own images on the internet e.g., on social networking sites
- In accordance with UAE Cyber Safety, parents / caregivers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution, and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images
- Written permission from parents or carers will be obtained before photographs of students are published on the school website.
- Students' work can only be published with the permission of the pupil and parents or carers.

Cyber Bullying

The school takes bullying very seriously and has robust procedures for identifying and dealing with it. Cyber bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability disability, age or religion. Students are taught about bullying as part of Moral Ed. Lessons and through yearly programs such as Internet safety day and Anti-Bullying awareness.

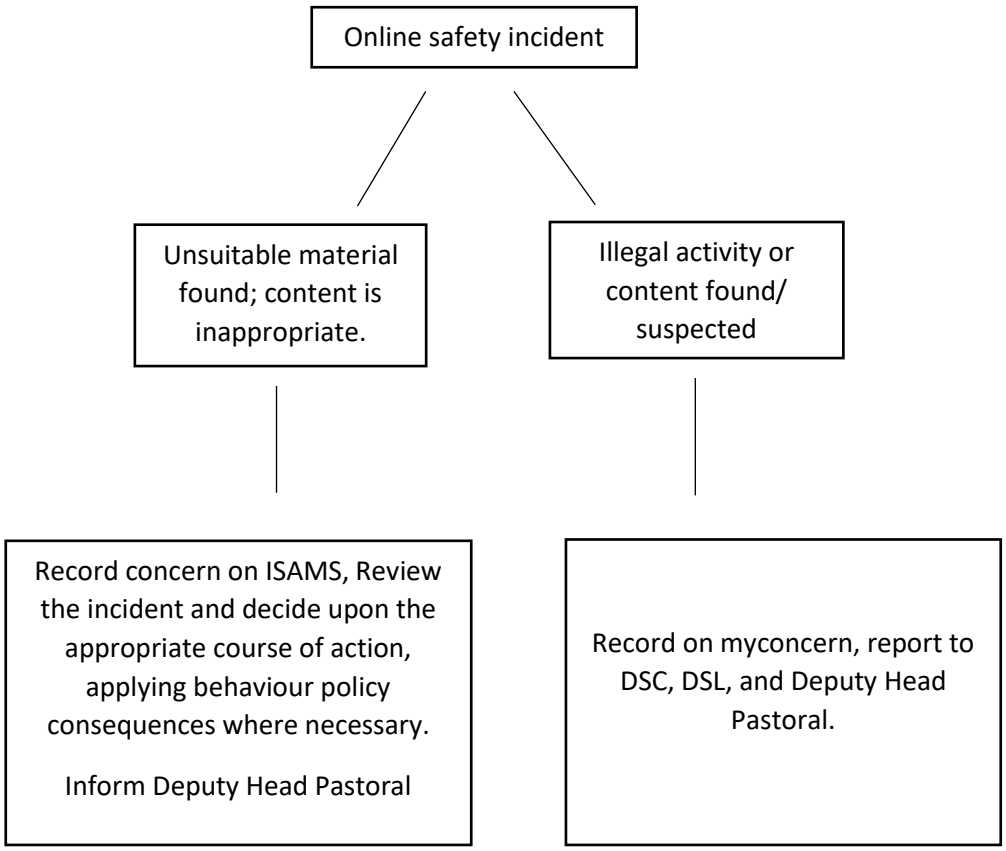
We expect all members of our community to communicate with each other with respect and courtesy. Bullying of any type will not be tolerated by the school and will be dealt with under the procedures within the Whole School Policies on Behaviour and Anti-bullying.

Linked Policies

Linked Policies	Safeguarding and Child Protection Policy Acceptable Use Policy Behaviour Policy Anti-Bullying Policy Staff Code of Conduct

Appendix 1

Referral Procedure



Appendix 2

Legislation

https://www.digitalwellbeing.ae/en/digital_laws_in_uae

https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws

https://u.ae/en/resources/laws

Cyber Privacy (source- https://www.digitalwellbeing.ae/en/digital_laws_in_uae)

Article 21:
It is illegal to invade someone's privacy by:

- Eavesdropping, recording, transferring conversations or communications, or materials
- Photographing others
- Publishing news, photos comments, or information even if true and correct
- It is essential to think carefully before acting online. Below are a few actions that may result in legal implications according to UAE's cybercrime law:
    - Sharing and posting photographs and media be careful before posting images that include other people without their consent. This is a criminal offence that breaches other people's privacy.
    - Privacy and confidentiality: disclosing private or confidential information about an individual or organization without consent can result in legal implications.
    - Offensive emoticons and emojis: Refrain from using culturally offensive emojis in social media conversations. This can result in serious complaints from the recipient even if it was intended as a joke.
- Defamation: or ruining an individual's reputation by sharing content that provokes public disapproval or contempt is a strict criminal offence.
- Immoral, offensive content that shakes social cohesion: any content that is "inconsistent with public morals and good conduct including content that is un-Islamic, blasphemous, lewd, that encourages sinful activity, or that is aimed at corrupting minors, etc." can have legal implications.
- Hacking and Malicious codes: "UAE TRA monitors online content available and prohibits content for hacking and malicious codes, Internet content providing unlicensed VoIP services and other illegal Internet content.

Appendix 3

Useful Links

- UK Safer Internet Centre. http://www.saferinternet.org.uk/
- UKSIC http://www.saferinternet.org.uk/
- Internet matters http://www.internetmatters.org/
- 'Safe to Learn' http://www.anti-bullyingalliance.org.uk/resources/safe-to-learn/#
- Kidscape – https://www.kidscape.org.uk/resources?gclid=CKP7g9DB0McCFY6RGwodJKEE5g
- CEOPS http://ceop.police.uk/
- Thinkyouknow https://www.thinkuknow.co.uk/
- Young Minds - http://www.youngminds.org.uk/?gclid=CLjctorC0McCFSQXwwoduRwLcw
- The Anti-Bullying Alliance http://www.anti-bullyingalliance.org.uk/
- Laws in the UAE- https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/uae