# Digital Safety Policy

Version Control

## for

## Stamford American International School

| | | |
|---|---|---|
| Author | Original Source: Cognita Asia - Linus Chiam Terence Lim Fiona Dixon<br>School Iteration: Director of Digital Learning, Head, IT Operations & Business Partnering | |
| Version Number | 03 | |
| Effective date | 01 November 2023 | |
| Next review date | 1. As and when needed by SAIS, or<br>2. Cognita next review date, as appropriate | |
| Changes from previous version | | |
| **Previous Version** | **Author** | **Effective Date** |
| | | |
| | | |
| **Approval** | | |
| SAIS Leadership Team | SAIS Leadership Team | 01 November 2023 |
| | | |

## Contents

## 1 INTRODUCTION AND PURPOSE

1.1 The use of technology as a tool has become an integral part of school and home life.

1.2 Stamford is committed to the effective and purposeful use of technology for teaching, learning and administration and is also committed to protecting its staff, students, parents and visitors from illegal or harmful use of technology by individuals or groups, either knowingly or unknowingly.

1.3 The school should actively promote the participation of parents to help the school safeguard the welfare of students and promote the safe use of technology.

1.4 This policy is available to staff, and the relevant sections are available to students, parents, and visitors on request.

1.5 It is the school's expectation that all staff are familiar with this Digital Safety Policy and follow its guidelines.

### Purposes of this document

1.6 To help students use technology safely and responsibly.

1.7 To help students enhance their learning, collaboration, and productivity.

1.8 To promote responsible use and care of technology and IT services available to staff, students, parents and visitors.

1.9 To outline the acceptable and unacceptable use of technology and IT services at the school, both on and offsite.

1.10 To outline the roles and responsibilities of all staff, students, parents, and visitors.

1.11 To educate and encourage students to make good use of the educational opportunities presented by access to technology at the school.

1.12 To safeguard and promote the welfare of students, by anticipating and preventing risks arising from, but not limited to:

- exposure to harmful or inappropriate material (such as pornographic, racist, extremist, or offensive materials).
- inappropriate contact from strangers.
- cyber-bullying and abuse.
- copying and sharing personal data and images.
- taking and use of photos, images, and videos of students.

1.13 To outline guidelines for reporting misuse of technology.

## 2 SCOPE

2.1 This policy applies to all staff, students, parents, and school visitors.

2.2 This policy applies to the use of:

- All technology devices and equipment connected to the school network, including personal devices.
- All technology devices supplied by the school to employees and contractors, both onsite and offsite.
- All technology devices supplied by the school to students via our 1-to-1 device programme, both onsite and offsite.
- All applications and IT services provided by the school for teaching, learning and administration; and
- All applications and IT services available online and accessible via the school network or a school technology device.

2.3 The school will take a wide and intentional approach to consider what falls within the meaning of technology. This policy relates to all technology, computing and communications devices, network hardware and software and services and applications associated with them, including, but not limited to:

- the school network, WiFi and Internet access;
- desktops, laptops, thin client devices;
- tablets, mobile (smart) phones, smart watches;
- digital devices for audio, still images and moving images (e.g., personal music players and GoPro devices);
- digital displays and smart boards;
- 2D and 3D printers;
- communication and collaboration applications (e.g., Email, Microsoft Teams, Google Meet);
- School Information Systems (SIS) and Learning Management Systems (LMS);
- mobile messaging apps (e.g., Snapchat and WhatsApp); and
- social media (e.g., Facebook, Instagram, Tik Tok).

2.4 This policy applies to any action by a member of the school community that might put the culture or reputation of the school at risk.

2.5 This policy applies to any member of the school community where staff, students, parents, or visitors are put at risk of harm.

## 3 RESPONSIBILITIES

3.1 This policy document is the responsibility of Stamford American International School. The Head of IT is responsible for publishing this policy and for the ongoing enforcement and monitoring of this policy at the school level.

3.2 All staff, students, parents, and visitors are responsible for adhering to the policy.

## 4 POLICIES

4.1 The school is committed to ensuring the safe and purposeful use of technology for teaching, learning and administration.

4.2 Staff, students, parents, and visitors are responsible for their actions, conduct and behaviour when using technology at all times.

4.3 The school will support the use of technology and make internet access as unrestricted as possible whilst balancing the educational needs of our students, the safety and welfare of staff, students, parents and visitors, and the security and integrity of our systems.

4.4 Monitoring, logging, and alerting tools are in place to maintain technology safety, safeguarding and security for the protection of staff, students, parents, and visitors.

4.5 Our students:

4.5.1 are responsible for following the Responsible Tech Use Guidelines, as agreed each academic year or whenever a new student starts at the school for the first. time, and are required to sign that they have read and understood the rules.

4.5.2 are taught to utilise the internet in a safe and responsible manner through Homeroom and advisory lessons, in alignment with the Common Sense Education scope and sequence.

4.5.3 are taught to immediately tell an adult about any inappropriate materials or contact from someone they do not know.

4.5.4 are made aware of the potential use of online digital technologies to expose young people to inappropriate contact from strangers and extremist ideas and know what to do if they encounter such issues.

4.5.5 are taught and encouraged to consider the implications of misusing the internet and, for example, posting inappropriate materials to websites.

4.5.6 are taught that the downloading of materials, for example, music files and photographs, needs to be appropriate and ‘fit for purpose’, based on research for schoolwork, and be copyright free.

4.5.7 are taught to understand what is meant by e-safety through age-appropriate delivery.

4.5.8 are taught that sending malicious or hurtful messages inside or outside of the school can become a matter whereby the school may set sanctions or involve outside agencies such as the police.

4.5.9 are taught not to put themselves at risk online or through mobile phone use and taught what to do if they are concerned, or if they have put themselves at risk;

4.5.10 are given explicit guidelines and procedures for using mobile phones and other personal devices in school and are expected to abide by these; and

4.6 If students or staff need to connect to the internet using a personal device, we encourage them to connect using the Stamford Guest network. Students should avoid using their personal devices' cellular data services to access the internet to ensure safety.

4.7 Any concern regarding unsafe or inappropriate use of technology should be reported as soon as possible to a teacher, divisional safeguarding lead, or Digital Learning Team. Depending on the nature of the concern, it may be escalated to the Designated Safeguarding Lead or an appropriate person on the Senior Leadership Team.

## The Right to Use School Network and Equipment

4.8 Staff, students will be allocated a unique username and password for accessing technology devices and services. Staff are required to set up 2 Factor Authentication to augment account security. Students in Grade 5 and younger are expected to sign in with their assigned password, while Grade 6 and older are required to create a strong, unique password for their account. Students are expected to keep their passwords private.

4.9 All school technology remains the property of the school. The school may reasonably request the device or withdraw access to the service at any time and, if applicable, the device must be returned to the school.

4.10 For cyber security reasons, only school-provided devices should connect to the Staff or Student networks. Personal devices may connect, but only to the Guest network. Where this is not practicable, exceptions may be granted after assessment and approval by the Head of IT.

4.11 Any attempt to access or use an unauthorised user account or email address by staff, students, parents, or visitors is prohibited.

## Appropriate Use of Technology for Digital Safety

4.12 The school provides systems and applications accounts to staff, students, parents, and guests as required. Users must:

- Not allow other people to use their user accounts.
- Not use someone else’s account.
- Lock their device or logout of their user accounts when not in use.
- Only use school applications and email for official School business
- Not send messages or emails from school accounts such that they appear to come from an individual other than the person sending the message.

4.13 The school provides technology (hardware and software) to support education and the running of the school business.

- Users of school technology equipment are expected to take care of the equipment through responsible behaviour.
- When staff and students are not using their devices, the screens should be locked to prevent unauthorised usage.
- Anyone who deliberately damages or abuses school equipment will be billed for the full replacement costs of the equipment.
- Do not:
  - Attempt to download or access illegal software on school devices.
  - Install school owned software on a personal device without written approval from the Head of IT.
  - Attempt to copy or remove software from a school-owned device.
  - Attempt to alter the configuration of the hardware equipment or any accompanying software unless instructed by the IT team.
  - Attempt to access data for which the user is not authorised.

4.14 The school endeavours to mitigate safeguarding and security risks associated with technology.

- The school has IT security systems in place to block access to unsuitable material and to protect the welfare and safety of staff, students, parents/guardians, and guests.
- The school has technology security systems in place to block and to protect against computer viruses or other malicious software such as spyware.
- Do not:
  - Try to bypass school IT security systems whilst using school devices or the school network.
  - Use software or network routing designed to bypass filters and access blocked sites.
  - Deliberately attempt to access inappropriate content (eg. obscene, illegal, hateful, abusive, offensive, pornographic, extremist or otherwise inappropriate materials) that may not be fully blocked by the security systems

4.15 It is the responsibility of all technology users to ensure the welfare of others and themselves, on both school and personal devices. These responsibilities are described in the Safeguarding and Conduct requirements.

- Students, staff and parents/guardians must not use their own or the school's technology to bully others.
- Students and staff must not create or share sexualised content, including images, audio, video, and/or text, on both school and personal devices, on school premises, or during school trips and activities.
- Students must not use school or personal devices to make contact or engage with people whom they do not know without parental or teacher supervision.
- Concerns regarding welfare associated with the use of technology should be reported to a teacher, member of the School Leadership Team or Designated Safeguarding Lead at the earliest opportunity.

4.16 The school supports the appropriate use of digital social media.

- Students should not use any social media for which they are under the legal age requirements (eg. 13 years old for Instagram and WhatsApp).
- Staff, students, parents, and visitors of the school must not make inappropriate online comments related to the Stamford Community or bring the school’s name and reputation into disrepute on any forum/platform.

- Staff should only connect with students using school accounts and official communication channels. Contact via personal phones, social media, or non-school messaging services is prohibited. Please see Code of Conduct (Section 7: Staff/Student Contact) for further details.

## School issued devices: Access & Privacy

4.17 Access to assigned devices and IT content:

- Students in the Elementary School have Apple Classroom installed on their iPads so that teachers may monitor classroom digital activity. For older students teachers are able to request the use of Apple Classroom for monitoring as needed.
- Students and Staff devices are installed with Chrome Remote Desktop so that IT can provide remote assistance. This is only used with the permission of the device assignee.
- Stamford reserves the right to access a school owned device and monitor its use and content under circumstances including but not limited to:
    - To detect and/or prevent crime.
    - To enable system security protection (e.g., Virus, Malware, Hacking, or other Risk).
    - To investigate potential misuse, abuse and/or illegal activity.
    - To monitor compliance with employment and statutory obligations.
    - To guarantee the integrity of the school devices, technology, and IT systems.

## Photographs, Images & Videos

4.18 Stamford abides by all relevant personal data protection legislation (Singapore PDPA and UK GDPR) and Stamford's data protection policy.

4.19 At Stamford, we understand that an image or video is considered personal data. Parents and guardians are asked during the admissions process if they choose to opt-out from use of their child's media in external, paid marketing. Those children are flagged in PowerSchool under "Marketing Photos Opt-out." Parents and guardians may withdraw this permission at any time by submitting a request on MyStamford. Stamford retains the right to use student media for internal or non-paid marketing purposes.

4.20 Students, parents and visitors must obtain consent before taking photos or videos of staff or students. Permission may be granted by the school in the event of performances/events organised by the school.

4.21 Staff are permitted to take school and learning-related photos or videos of students and other staff for internal use, with consent. If they take photos or videos using a personal device, they are required to remove those media from any local storage or personal accounts within one week.

4.22 When the school grants consent, parents are asked to be considerate when taking videos or photographs at school events. They are requested not to publish material of children other than their own in any public forum without the consent of the relevant family. It is illegal to sell or distribute recordings from events without consent. Any parent who does not wish their child to be videoed or photographed at school events by other attendees must notify the school in advance and in writing.

4.23 Photos, images, and videos intended for teaching and learning, administrative, school prospectus, performance purposes, after school or off campus activities, and other school-related purposes should be retained only for the duration necessary to serve their intended purpose. Furthermore, we should ensure that any retention is consistent with the legitimate interests of the school and that such interests are not overridden by the rights and freedoms of the individuals involved. When there is no longer a legitimate interest or purpose, the images should be promptly deleted. Any photo, image, or video retention longer than 5 years must be approved in writing by the Head of IT. This approach fosters responsible data management and respects the privacy of individuals while serving the educational mission effectively.

4.24 The staff Annual Safeguarding Declaration includes a statement saying that any photos or videos residing on personal devices have been deleted from the device and personal cloud storage. Staff must comply and sign off on this at the start of every school year.

4.25 IT will email Staff toward the end of each semester to delete all images from personal devices and cloud storage.

## 5 PROCEDURES FOR REPORTING

5.1 Staff who witness a concern, incident, or unsuitable media regarding technology should take the following actions:

- Attempt to stop or minimize the problem.
- Prevent exposure of the incident to others.
- Record the nature of the incident and those involved.
- Preserve evidence to enable investigation if required.
- Report the incident or concern to the Designated Safeguarding Lead or IT Team as appropriate (through a Self Report).

5.2 Any students, parents, or visitors of the school who witness a concern, incident, or unsuitable media regarding technology should report the incident immediately to a teacher or staff member.

5.3 Concerns regarding viruses and other malicious software on a school device or on the school network should be reported to a member of the IT Team at the earliest opportunity.

5.4 Loss, damage, or theft of school technology should be reported to a member of the IT Team at the earliest opportunity.

5.5 Students must take responsibility for their use of IT equipment both at school and at home; should parents or guardians have concerns or become aware of an issue, they should communicate those concerns with the school so we can offer advice and support.

## 6 REMOVAL OF NETWORK ACCESS/SANCTIONS

6.1 Anyone found abusing the Digital Safety Policy may have their technology rights removed and may be subject to further disciplinary action.

6.2 The school may inform the police or other law enforcement agency in the event of any digital use that could be regarded as potentially illegal.

## 7 POLICY MONITORING AND REVIEW

7.1 The school takes its responsibilities in relation to digital safety and use of technology by staff, students, parents, and visitors seriously and understands the importance of monitoring, evaluating, and reviewing its policies and procedures regularly.