E-Safety, Devices & Technology Policy

Straits International School, Rawang

Approval date	September 2021	**Review Date**	September 2023
Review Cycle	Every 2 years		
Scope	**Whole school**		•
	Secondary school		•
	Primary school		•
	EYFS		•
Ownership		**Approved by**	CP and SLT

Part of International Schools Partnership®

Table of Contents

Objectives

Straits International School uses instructional technology as one way of enhancing our mission to teach the skills, knowledge and behaviors students will need as responsible citizens in the global community. Students learn collaboration, communication, creativity and critical thinking in a variety of ways throughout the school day. SIS also recognises that digital technology enables personalised learning tailored to students' particular needs and interests and transforms assessment, reporting and feedback, driving new forms of collaboration and communication.
In an effort to increase access to those 21st Century skills, SIS will also allow students to use their Chromebooks (KS2-4) Primary students to bring in personal devices on our student network and on school grounds, provided they follow the rules and guidelines outlined within this policy, as well as sign the Acceptable Use Agreement document (attached).

Purpose of this policy

To ensure that all students and members of our school community understand:

- Our commitment to providing students with the opportunity to benefit from digital technologies to support and enhance learning and development at Straits International School.
- Expected student behaviour when using digital technologies including the internet, social media, and digital devices (including computers, laptops, tablets)
- The school's commitment to promoting safe, responsible and discerning use of digital technologies, and educating students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and digital technologies
- Our school's policies and procedures for responding to inappropriate student behaviour on digital technologies and the internet

Safe and appropriate use of digital technologies

Digital technology, if not used appropriately, may present risks to users' safety or wellbeing. At Straits International School, we are committed to educating all students to be safe, responsible and discerning in the use of digital technologies, equipping them with skills and knowledge to navigate the digital age.

At Straits international School, we:

- use online sites and digital tools that support students' learning, and focus our use of digital technologies on being learning-centred
- supervise and support students using digital technologies in the classroom

- effectively and responsively address any issues or incidents that have the potential to impact on the wellbeing of our students
- educate our students about digital issues such as online privacy, intellectual property and copyright, and the importance of maintaining their own privacy online
- actively educate and remind students of our Behaviour policy that outlines our School's values and expected student behaviour, including online behaviours
- have an Acceptable Use Agreement outlining the expectations of students when using digital technology at school
- use clear protocols and procedures to protect students working in online spaces, which includes reviewing the safety and appropriateness of online tools and communities, removing offensive content at earliest opportunity
- educate our students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and other digital technologies
- provide a filtered internet service to block access to inappropriate content
- refer suspected illegal online acts to the relevant law enforcement authority for investigation
- support parents and carers to understand safe and responsible use of digital technologies and the strategies that can be implemented at home.
- All students will be required to sign the Acceptable Use Agreement along with their parents/guardians at time of enrolment.
- It is the responsibility of all students to protect their own password and not divulge it to another person. If a student or staff member knows or suspects an account has been used by another person, the account holder must notify the teacher or technology manager as appropriate, immediately.

All messages created, sent or retrieved on the school's network are the property of the school. The school reserves the right to access and monitor all messages and files on the computer system, as necessary and appropriate. Communications including text and images may be required to be disclosed to law enforcement and other third parties without the consent of the sender.

Chromebooks

Students must adhere to the above outlined guidelines and rules for safe and appropriate use of digital technology. The following guidelines are specifically for use of Chromebooks.

Key Stage 2 & 3

Key Stage 3 students must follow these rules when using their Chromebooks in school:

- Students are allowed to decorate their Chromebook with stickers etc. as long as they are school appropriate.
- Students are allowed to personalise their home screen, as long as it is school appropriate.
- Chromebooks are only to be used in the classroom or in the designated area in the library (no Chromebooks in the corridors, canteen or roof).
- Students are not allowed to play games on their Chromebooks, unless these are educational games that have been vetted by the teacher.
- Students are not allowed to watch YouTube videos, movies or any other types of media on their Chromebooks, unless these have been prescribed by the teacher.
- Students must lower their Chromebook screens when the teacher is talking, and must not continue to use their device.
- Email, comments or chat must be limited to the lesson content and school appropriate
- Students must charge their Chromebooks before coming to class
- Students are responsible for their own Chromebooks, including warranty and safekeeping.
- Consequences for misuse of Chromebook (subject to severity of offence)
    - Verbal warning given
    - Confiscation of Chromebook for lesson/rest of the day and parents/guardians informed
    - Confiscation of Chromebook and given to the Head of Secondary for the rest of the week and parents/guardians informed.
    - Consequences outlined in Behaviour and Anti-Bullying policies also apply.

Key Stage 4

Students in Key Stage 4 must also adhere to the general rules applicable to Key Stage 3. However, they are awarded the following additional privileges:

- KS4 students are allowed to use their Chromebooks around the school (other than classrooms and the library).
- KS4 students are allowed to listen to music on their Chromebooks during independent study or when given expressed permission by the teacher, using headphones, as long as the music as at an acceptable volume and is appropriate (no explicit lyrics)

Any abuse of the above allowances, or flouting of rules, will result in loss of privileges, or confiscation of Chromebooks.

IPADs

EYFS & Key Stage 1

Children in EYFS and KS1 have access to a school set of IPADs. These IPADs are property of the school and cannot be taken home by the children for any reason. No apps may be downloaded onto the IPAD without prior approval. Class Teachers and Teaching Assistants are responsible for ensuring that the IPADs are taken care of and stored and charged properly. No child should be left alone unsupervised while using an IPAD.

In some cases, students have been permitted to bring their own device to school (BYOD):

Guidelines:

- Students and parents/guardians participating in B.Y.O.D. must adhere to the Student Code of Conduct, Student Handbook and, Acceptable Usage Agreement.
- Each teacher has the discretion to allow and regulate the use of personal devices in the classroom and on specific projects.
- Approved devices must be in silent mode while on school campus, unless otherwise allowed by a teacher. Headphones may be used with teacher permission.
- Devices may not be used to cheat on assignments, quizzes, or tests or for non-instructional purposes (such as making personal phone calls and text messaging).
- Students may not use devices to record, transmit, or post photographic images or video of a person or persons on campus during school hours or during school activities, unless otherwise allowed by a teacher.
- Devices may only be used to access computer files on internet sites which are relevant to the classroom curriculum.

Students and Parents/Guardians acknowledge that:

- The school's network filters will be applied to a device's connection to the internet and any attempt to bypass the network filters is prohibited.
- Straits International School is authorized to collect and examine any device that is suspected of causing technology problems or was the source of an attack or virus infection. Students are prohibited from:
    - Bringing a device on premises that infects the network with a virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information.
    - Processing or accessing information on school property related to "hacking." Altering or bypassing network security policies.
- Students and parents should be aware that devices are subject to search by school administrators if the device is suspected of a violation of the student code of conduct. If the device is locked or password protected the student will be required to unlock the device at the request of a school administrator.
- Printing from personal devices will not be possible at school.
- Personal devices must be charged prior to school and run on battery power while at school.

Lost, Stolen, or Damaged Devices:

Each user is responsible for his/her own device and should use it responsibly and appropriately. Straits International School takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. While school employees will help students identify how to keep personal devices secure, students will have the final responsibility for securing their personal devices.

Student behavioural expectations

When using digital technologies, students are expected to behave in a way that is consistent with SIS's values of learning respect and empowerment, Safeguarding policy, and Anti-Bullying policy. When a student acts in breach of the behaviour standards of our school community (including cyberbullying, using digital technologies to harass, threaten or intimidate, or viewing/posting/sharing of inappropriate or unlawful content), Straits International School will institute a staged response, consistent with our policies.

Breaches of this policy by students can result in a number of consequences which will depend on the severity of the breach and the context of the situation.
This includes:

- removal of network access privileges
- removal of email privileges
- removal of internet access privileges
- removal of printing privileges
- other consequences as outlined in the school's Safeguarding and Anti-Bullying policies.

Mobile Phones (Staff) and E Safety tips for staff

SIS has a strict no mobile phones policy when around children. In lessons, CCAs, duty time etc. (any environment where there are children around), staff are forbidden from using their phone for personal use. In the case of taking photos for school purposes, staff are permitted to use their mobile phones, however, all photos of children must be deleted immediately after and photos uploaded to a secure school server. When walking around the school, please also refrain from using your mobile phone except when absolutely necessary. Personal phone calls etc. should be taken during break time in a classroom or space where there are no children around.

- Reminders for staff: Posting any photos of the children on staff's own social media is forbidden.
- If you are sharing photos on a school supported official site, please ensure that prior permission from parents has been obtained.
- Not being friends on social media with students
- Using the school's secure log on system to access the school system
- Only using the school email system or Class Dojo to contact parents and children
- Ensure they do not access inappropriate websites in school or expose children to inappropriate material
- Report any concerns to the DSL.

Promoting E-safety and awareness about possible dangers

Gaming

Just like films games are becoming more realistic with dialogue and scenes these have age limits despite this games are often mentioned by children as to what they have seen/played if you are aware of this under age use you should report it to your DSL.

Minecraft – PEGI 7+ but online 13 +
Fortnite – PEGI 12 +
Fifa – PEGI 7+
FORZA – PEGI 12 +
COD/Battlefield/GTA – PEGI 18 or R rated

Trolling

Trolling is when an individual (or group) posts offensive and hurtful messages online, such as on social network sites, chat rooms, online forums or blogs etc, with the intent of upsetting others.

Grooming

Grooming used to be a complex activity requiring manipulation of the child and their environment – this has been simplified by technology (available 24/7), ease of access to children through IT communications, naivety of parents, carers and protectors and the availability of a number of social networking sites

- Grooming process may take minutes, hours, days or months
- Groomers remain at different phases depending on the dynamics between their goals, needs or style and the reactions of the young person
- Offenders tend to use what worked previously
- Use a wide range of internet facilities to contact young people
- Use multiple identities
- Use blackmail (sextortion)
- No 'one size fits all' – range and fluidity of behaviours

Sexting

- This relates to the issue of sending or posting sexually suggestive images including nude or semi-nude photographs via mobiles or over the internet

- In all cases where an incident of youth produced sexual imagery is noticed by staff or reported to staff by children the incident should be reported to the Designated Safeguarding Lead as soon as possible.

Cyberbullying

'Cyberbullying is bullying that takes place over digital devices like mobile phones, computers, and tablets. Cyberbullying can occur through SMS, text and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behaviour.'
The most common places where cyberbullying occurs are:

- Social Media sites such as Facebook, Instagram, Snapchat and Twitter
- SMS (Short Message Service) also known as text messages sent through devices
- Instant Message (via devices, email provider services, apps and social media messaging features)
- Email

Remember cyberbullying happens 'in and out of the school gates'. It doesn't stop at the end of the school day, it can happen 24 / 7 in a child or young person's own bedroom and can have an audience of millions.

Last review date: September 30th 2021