SWISS INTERNATIONAL SCIENTIFIC SCHOOL DUBAI

Acceptable Use Policy
Whole School

DATE:	June 21 2023
REVIEW DATE:	June 21 2024
Owner:	ICT Department
Version Number:	Version 01

Contents

1. Introduction

Information and communications technology (ICT) is an integral part of the way our schoolwork's and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors.
- Establish clear expectations for the way all members of the school community engage with each other online.
- Support the school's policy on data protection, online safety and safeguarding.
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems.
- Support the school in teaching pupils safe and effective internet and ICT use.
- This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary policy.

2. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose.

- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

3. Unacceptable use

The following is considered an unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/live streams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities

- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Principal and ICT Team Lead will use professional judgement to determine whether any act or behaviour not on the list above is considered an unacceptable use of the school's ICT facilities.

3.1. Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on staff disciplinary/staff code of conduct policy. This can be found in the public SharePoint - HR policy.

4. Staff (including governors, volunteers, and contractors)

4.1. Access to school ICT facilities and materials

The school's ICT Team Lead manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT Team Lead.

4.2. Use of phones and email

- The school provides each member of staff with an email address.
- This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email accounts.
- All work-related business should be conducted using the email address the school has provided.
- Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email accounts.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the UAE Data Protection Law 2022 in the same way as paper documents.
- Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- If staff send an email in error that contains the personal information of another person, they must inform the Data Protection Officer immediately and follow our data breach procedure.
- Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.
- School phones must not be used for personal matters.
- Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT-acceptable use as set out in **Appendix 2**.

4.3. Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Principal and ICT Team Lead may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during [contact time/teaching hours/non-break time]
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes
- Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos or photos).

Staff should be aware that the use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

4.4. Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is always appropriate.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see Appendix 1)

4.5. School social media accounts

The school has an official Facebook/Instagram/Twitter/LinkedIn page, managed by the marketing department. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account. The access is strictly limited to the Marketing department only.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they always abide by these guidelines.

4.6. Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record, and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime

5. Students

5.1. Access to ICT facilities

Computers and equipment in the school's ICT suite are available to students only under the supervision of staff.

5.2. Acceptable Use for Students

- Each student must use SISD systems and networks in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the ICT systems and other users. For each student's own personal safety, they will:
- Be aware that SISD will monitor their use of ICT systems, devices and digital communications.

- Keep the username and password safe and secure – they will not share it, nor will they try to use any other person's username and password. They will not write down or store their password where it is possible that someone may steal it.
- Be aware of "stranger danger" when communicating online.
- Not disclose or share personal information about themselves online (this includes names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- Students should not meet with people off-line that they have communicated with online.
- Immediately report any unpleasant or inappropriate material or messages or anything that makes them feel uncomfortable when viewed online.
- Ensure that they have permission to use the original work of others in their own work.
- Where work is protected by copyright, students should not try to download copies (including music and videos)

5.3. School Network and System

- Accessing data, a server, or an account for any purpose other than conducting school Business, even if a student has authorized access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- When they are using the internet to source information, they should take care to check that the information they access is accurate, as the work of others may not be truthful and may be a deliberate attempt to mislead. Reference should be made to the Academic Honesty Policy.
- SISD has the right to take action against the student if they are involved in incidents of inappropriate behavior, that are covered in this agreement, when they are out of school and where they involve their membership of the school community (examples would be cyberbullying, use of images or personal information)

5.4. Security and Personal Safety

The school will monitor the use and impact of the AUP and BYOD policy by:

1. Keeping a log of any reported incidents of inappropriate use.
2. Monitoring internet use and teaching children digital citizenship.
3. Generating feedback from parents and students through use of questionnaires and surveys.
4. Continue to share successful device integration practice amongst teachers.

The BYOD policy agreement can be found in **Appendix 3.**

SISD has a responsibility to maintain the security and integrity of the technology it offers its students and to ensure the smooth running and operation of SISD:

• In order to use IT the facilities of SISD a student must first be provided with their own username and password by ICT services. Registration to use the computer facilities implies, and is conditional upon, acceptance of this Policy.

• All individually allocated usernames and passwords are for the exclusive use of the student to whom they are allocated. Passwords protect SISD's systems from access by unauthorized people; they protect the student's work and SISD's information. The student is personally responsible and accountable for all activities carried out under their username.

• The password associated with a particular personal username must not be divulged to another person. Attempts to access, or use, any username or other data, which is not authorized to the student is prohibited.

• Students will not install or attempt to install or store programs of any type on any school device, nor will they try to alter computer settings.

5.5. Equipment

• SISD's systems and devices are primarily intended for educational use and are not to be used for personal or recreational use. For the avoidance of doubt written permission must be from a member of the teaching staff.

• Downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work are prohibited.

• Systems and devices used for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting are prohibited.

5.6. Cyber Bullying and Social Media

In accordance with the SISD Whole School Behaviour Policy, the use of and participation in social media outlets and/or forums should:

• Demonstrate respect for the members of the school community (including all students and personnel).

• Not breach confidentiality, defame, or make threats to any person in the school community.

5.7. Mobile Device Monitoring

In accordance with the SISD Whole School Behaviour Policy, the use of mobile phones and smart watches and related communication apps (Whatsapp, Twitter, Instagram etc.) is prohibited during school hours. The behaviour policy will be applied should a student be in breach of this. This may include the use of communication platforms outside of school hours.

6. Boarding Students

The guidelines for Acceptable Use during the school day, still apply during after school hours in the boarding houses. Boarding students Additionally the below guidelines apply.

6.1. Mobile Phone Usage

- Boarding students are permitted to have one mobile phone in their possession. All mobile phones must be registered with the boarding team.
- Boarding students must provide their UAE mobile number to the boarding team for use in the case of an emergency.
- Grades 6 – 8 students will have access to their phones for short periods of time as below. At all other times, the mobile phones will be stored in the boarding administration office:
    - Before the school day between 06:30 – 07:20
    - After the school day from 15:30 – 16:40
    - Before bed time from 20:00 – 21:00
- Boarding student's mobile phones may be confiscated in line with the Boarding Positive Behaviour Policy.

6.2 Microsoft Teams

- Microsoft Teams is an essential means of communication for both boarding staff and boarding students.
- Boarding students are required to have Microsoft Teams downloaded to their mobile phone in order to be contactable at all times.
- All boarding student Microsoft Teams users are expected to adhere to the generally accepted rules, particularly in relation to the use of appropriate language.
- Boarding students must be respectful of appropriate and acceptable times at which to message a boarding staff member. It is generally acceptable to message between 06:00 – 20:00, and in the case of an emergency.

6.3 Orah

- Orah is the SISD Boarding Management Information System.
- Parents, and students have their own individual log ins to the system.
- At no time should parent log ins be shared with students. This is deemed as a breach in safeguarding procedure and policy.
- All boarding students must have Orah downloaded to their mobile phones for roll calls and exeat permissions.

6.4 Boarding Televisions, Streaming Sites and Online Gaming

- The boarding common rooms are equipped with television screens and gaming equipment.
- Students are not permitted to install, or download applications to the televisions or gaming equipment, without the approval from the Head of Boarding.
- All necessary installations will be carried out by the school ICT team.
- Approved streaming sites have been installed on the televisions, with a boarding ID login. Students must not log out of these accounts, r use these accounts in any unacceptable way.

7. Parents

7.1. Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the PFC) may be granted an appropriate level of access or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2. Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

8. Data Security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It, therefore, takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot

guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure and enable multifactor authentication.

All users are enforced to change their password every 90 days.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

8.1. Software updates, firewalls and anti-virus software

All the school's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

8.2. Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

https://sisd.ae/privacy-policy/

8.3. Access to facilities and materials

- All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.
- These access rights are managed by ICT Department.
- Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert ICT Department immediately.
- Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access.

9. Protection from cyber attacks

Please see the glossary (**Appendix 4**) to help you understand cybersecurity terminology.

The school will:

Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure.

Provide training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:

- Check the sender address in an email
- Awareness about phishing, smishing attacks.
- Respond to a request for bank details, personal information or login details
- Verify requests for payments or changes to the information

Make sure staff are aware of its procedures for reporting and responding to cyber security incidents.

Investigate whether our IT software needs updating or replacing to be more secure

Put controls in place that are:

- **'Proportionate'**: the school will verify this using a third-party audit (such as VAPT testing twice a year - at least annually], to objectively test that what it has in place is up to scratch
- **Up-to-date:** with a system in place to monitor when the school needs to update its software.

Backup of critical data is being taken on a daily basis to a Network Attached Storage (NAS) in the server room. The backup of the backup-NAS is being taken to another secondary NAS in another building.

Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider.

Make sure staff:

- Enable multi-factor authentication where they can, on things like school email accounts and, other school applications.
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- A nest generation firewall in place that is switched on with High Availability.
- Endpoint Detection and Response (EDR) solution in place

10. Internet Access

The school's wireless internet connection is secured. The Wi-Fi 6 with 802.11ax standard enables the stakeholders to access the network using the Active Directory credentials.

Proper filtering is in place to ensure that the stakeholders use the internet in a safe and secure way.

The staff, students and guest networks are separated, and separate policies are defined in the firewall.

10.1. Students

The Wi-Fi signal is available across the campus and the students can connect to the Wi-Fi using their email and password. Strict filtering is in place for the student's Wi-Fi network.

10.2. Parents and Visitors

Parents and guests can connect to the Guest Wi-Fi by putting the guest Wi-Fi codes provided by the front desk executives. Each parent/guest will have a unique code which will have a validity for a certain period.

11. Monitoring and Review

The principal and ICT Team Lead monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

The policy will be reviewed every 1 year.

12. Related Policies

This policy should be read alongside the school's policies on:

- Digital safety
- Safeguarding and child protection
- Staff discipline
- Data protection
- Mobile phone usage

Appendix 1: Facebook cheat sheet for staff

10 rules for school staff on Facebook

Don't accept friend requests from pupils on social media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages

Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Mobile Phone Usage Policy

Mobile and SIM card use policy

Mobile Tel. No.:	
Device Model:	
Issued To:	
Designation:	
Department:	
Date	

Purpose

This mobile device & Sim card (s) is provided for official state business use and may be made available to employees in positions where the associated benefits justify the additional operating needs.

Policy/Guidelines

1. The mobile device is the property of Swiss International Scientific School with a limited package of xxx free minutes of local calls, xxx local SMS & xx GB Data per month and should normally be used for legitimate business

purposes only and mobile devices may be used by designated users/department only.

2. Use for any other purpose (except in a genuine emergency) may cause the device to be withdrawn and subject the user to disciplinary action. SISD will monitor usage on regular basis including personal usage.
3. It may be necessary from time to time to make a personal call or send a personal text message. Users will be required to identify such personal use from the associated monthly invoice and will be expected to pay for this use at the relevant tariff, by means of cash payment or direct salary deduction.
4. Users must not use, try to use, or let anyone else use staff mobile communications devices for:
5. Anything that is illegal or immoral.
6. Making offensive, threatening, or harassing calls
7. Use of the Short Message System (SMS), multi-media messaging or email to send or receive inappropriate or offensive remarks, graphics, or images.
8. Mobile communications devices should be securely stored when not in use.
9. Users may be liable for repair or replacement costs, should their handset be damaged or lost. Any such damage should be reported to the IT Department and to the HR Department.
10. All losses of mobile data devices must be reported to the ICT Department & HR immediately.
11. The IT Department should be contacted as soon as possible within working hours to report the loss, in order that a replacement SIM can also be arranged.
12. Any member of staff who is due to leave/terminate contracts with SISD must return any mobile device and the Sim Card (s) to the ICT Department.
13. SISD reserves the right to withdraw this Mobile Device at any given time.

I acknowledge the receipt of the mobile device with sim card (s) from SISD and as I read, I have been informed and understand the content, requirements, and expectations of the mobile policy, I have received a copy of this document, and agree to abide by the policy guidelines.

Signed:	**Date:**

Appendix 3: BYOD Policy

Bring Your Own Device (BYOD) Policy and Agreements

Technology is a key part of education. To be able to live, learn and work successfully in an information-rich society, everyone, including our students, must be able to utilize technology effectively. It can provide our students with ubiquitous access to information and resources, enabling them to pursue their interests and learning needs in a much more personalised way. This does not mean that traditional approaches to education are no longer relevant, or used at our school. Rather, we are looking to utilize the potential of technology as a tool to enhance our learning environments. Our philosophy is that technology can be used to enrich and personalise the learning experience for all of our students.

With many SISD students owning their own device (laptop, tablet, etc.) for personal use, we have recognized the need to encourage students to utilize technology in a seamless fashion for educational purposes when they are at school. Under this approach, teachers will have the option to adopt a BYOD approach in their own classroom. How and when these devices will be used will be under the direction of your child's teacher, who will consult with the Deputy Head (Academics) on effective use of technology as a learning tool.

- In PYP teachers will provide you with specific details about this, including which days of the week/periods of time they would like the students to bring their device. For students who do not own a personal device we will have access to technology resources within the school and allow for collaboration when using devices. Teachers will plan lessons where devices can be used as an additional tool for learning.
- In PYP The choice of whether students bring a device from home will be that of the parents/guardians. Students may either bring a laptop or tablet device (guiding specifications are included in this policy); students may not bring a mobile phone for this program. Students are not encouraged to have games on these devices; the primary purpose of these devices at school is for them to act as a learning tool. Students who do not use them for this purpose may lose the right to bring their device to school for a period of time. While at school, these devices will only be kept in the classroom (which will be locked when the teacher is not present). In accordance with the school policy, students will not be allowed to take their devices with them during break times.

- In MYP and DP all students are required to have a fully charged laptop in school at all times to facilitate their learning.

When using their device students will be provided access to a filtered Internet connection that will enable them to do research and to collaborate and communicate with their peers in a safe manner. At the same time, we have measures in place to ensure that students do not misuse this system. Students and parents are requested to be aware of the expectations surrounding BYOD, which are outlined below. All students must without fail adhere to the Acceptable Use Policy.

Expectations:

1. Students will only use the technology appropriate, and at the teachers discretion.
2. Students will only use appropriate educational applications on their device (i.e. not games and/or non-school related tasks and functions) unless they have specific staff permission.
3. Students are not to call, text message, email, or electronically communicate with others from their personal device (including other students, parents, guardians, friends, and family) during the school day without permission from their teacher/s.
4. Students are permitted to only access the school's network through their personal devices. They are not allowed to access private networks when on campus. Students who use private networks (3G, 4G, hotspot, etc.) at school to access inappropriate information will face disciplinary action.
5. The student is solely responsible for any equipment that he/she brings to school. SISD is not liable for damaged, lost, or stolen equipment.
6. When students use technology inappropriately while on the school network, the same consequences will apply as the current IT policy apply, regardless of who owns the device.
7. SISD staff members (including IT staff) are unable to provide any major technical support for personal devices at school.
8. Students will receive guidance on use of personal devices from the class teacher.
9. Any lost, theft or change of ownership of the device will be reported.
10. Students will use a pass code that is kept confidential for their own personal device.

11. Students will be mindful of the times they contact staff. I.e. Not after 6pm or at weekends.

The school will monitor the use and impact of the BYOD policy by:

5. Keeping a log of any reported incidents of inappropriate use.
6. Monitoring internet use and teaching children digital citizenship.
7. Generating feedback from parents and students through use of questionnaires and surveys.
8. Continue to share successful device integration practice amongst teachers.

Students utilizing this opportunity to its fullest capacity within school expectations will find numerous benefits to instruction, resources, completion of assignments and personal organization. Students not following expectations for use of personal devices will face school disciplinary measures and lose the privilege to utilize personal devices in school for a period of time equal with the nature of the infraction.

Guideline Tablet Specifications

The following chart should help you in selecting and purchasing a tablet for your child to use. While there are many options, there are minimum specifications the students should have in order to effectively support your child's learning.

Machine Type	Tablet
Screen Size	7 inches or greater
RAM	4GB or Higher
Hard Drive	16 GB or Higher
Wireless	802.11g or Higher
Ports	Audio in/out, In-built microphone

Guideline Laptop Specifications

The following chart should help you in selecting and purchasing a laptop for your child to use. While there are many options, there are minimum specifications the students should have in order to effectively support your child's learning.

Machine Type	Laptop
Platform	Windows/Mac
Screen Size	13 inches or more
Processor	Intel corei3 or Higher AMD Athlon II or Higher
RAM	4 GB or Higher
Hard Drive	160 GB or Higher
Operating System	Windows 7 Professional or Higher, Mac OSX or Higher Must support English
Wireless	802.11g or Higher
Ports	2 USB ports, Audio in/out, In-built microphone, HDMI.
Battery Life	4+ hours (6+ cell or higher)

BYOD Agreement

Please read the information below, discuss this with your child and complete the form at the end of the document.

The school encourages all students to become familiar with the use of information technology. Parents/ guardians are encouraged to contact the appropriate personnel at the school if they require more information about this form.

Student

I understand that the school's computer network can connect me to useful information. While I have access to the computer network, I will follow all rules as stated in the school's computer usage policy. I hereby agree to the following while using the Internet and other information technology services:

I WILL

- Only use my device for the purpose directed by my teacher in charge.
- Use the Internet at school for educational purposes.
- Respect the rights and privacy of other users.
- Report any security issues that I may discover.
- If I accidentally come across something that is illegal, dangerous or inappropriate, I will clear my screen and immediately and quietly inform my teacher.

I WILL NOT

- Attempt to access and view any inappropriate material.
- Threaten, abuse or harass any other user.
- Send any inappropriate messages or emails.
- Send any anonymous or falsely addressed emails or messages.
- Use social media such as Facebook, Twitter, Discord or Instagram when at school.
- Download or print information without the permission from my teacher.
- Use chat channels while on school premises.
- Attempt to change or tamper with the computer network in any way.
- Attempt to bypass security systems in the school.
- Disclose my home address, telephone number or any credit card or pin number.

I understand that if the school decides that my child have broken this agreement, they may be prevented from using the school's computers or network for a period of time.

Please click here to confirm that you have read this policy

Appendix 4: Glossary of cyber security terminology

term	definition
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can

term	definition
	adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.

term	definition
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.