Tanglin Technology and E-Safety Policy

Overview

This Policy sets out who in the organisation will have access to the internet through the school network and how that access will be managed, along with the associated risks. It should be read in conjunction with the Student Code of Conduct; Student Misbehaviour and Sanctions Policy; Anti-Bullying Policy; Child Protection Policy; Personal Data Protection Policy and the Photo and Video Policy.

Further guidance for Staff use of Information Technology is available on the Staff Portal. In particular staff should be aware of:
The Staff Handbooks (Including the Code of Conduct for Staff and Guidance on Staff use of ICT and the Internet); Communications Guidelines and Protocols (including the 'Email Policy and Communications to Parents' and 'Social Media Protocol').

This Technology Policy has been agreed and approved by the Leadership Team and the Education Sub-committee of the Board of Governors (ESC). It will be reviewed annually by the Technology Working Group (TWG), chaired by the Director of Educational and Business Technology (EBT).

Contents

1. E-Safety

E-Safety refers to the safe and responsible use of all internet technologies and electronic communications such as computers, laptops, mobile phones, iPads and any other handheld device that students might access.

This policy highlights and reinforces the need to educate students about the benefits and risks of using technology, provides safeguards and raises awareness for users to enable them to control their online experiences. Each school has clear, age appropriate 'Responsible Use' guidance, which is shared and regularly reinforced with students (see Appendix 1)

This policy will operate in conjunction with other school policies including those for ICT, Behaviour, Bullying, PSHCE and Child Protection.

2. Teaching and Learning

2.1 How does technology support teaching and learning??

Our vision for the use of Technology at Tanglin is as follows:

Tanglin Trust School embraces new technology wherever it supports our mission. Staff are confident users of technology and are encouraged to be innovative. Students use technology to inquire, communicate and safely take risks. When they move on from Tanglin, they are confident users of current technology in a range of contexts, understanding the benefits, limitations and risks associated with its use.

A range of IT devices, software and internet based resources are used to support teaching and learning across the school where they enrich the learning experience, for example by:

i. Improving access to the curriculum
ii. Encouraging collaboration between students
iii. Enhancing communication by enabling multimedia approaches
iv. Enabling authentic student research
v. Supporting student self-management and organisation

2.2 How does the access to the internet support teaching and learning?

Benefits of using the internet in education include:

i. Access to up to date information from a wide variety of sources
ii. Access to online educational resources
iii. Educational and cultural exchanges between students world-wide
iv. Access to experts in many fields for students and staff

2.3 How will internet access be managed within the school ?

The school internet access has been designed for student and staff use and will include filtering appropriate to the age of the students and the needs of staff.

Students will be taught what internet use is acceptable and what is not and will be given clear objectives for it safe use.
Staff will guide students in online activities that will support the planned learning outcomes, with due regard for the students' age and maturity.

Students will be educated in the skills of Digital Literacy i.e. the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. Students will be taught to acknowledge the source of information and to respect copyright when using internet material in their own work.

Infant and Junior internet access must be approved and will be supervised at all times.
Senior students will be provided access according to requirements

All use should be in accordance with the relevant schools' Responsible Use Guidelines which form part of this document.
Students must follow the procedure for reporting unsuitable internet content.
This procedure will be shared with all students by their class teachers as part of the curriculum (see Appendix 1).

2.6 How will e-safety issues be handled?

Any breach of the Responsible Use Policy, or the Student Code of Conduct will be dealt with according to the Misbehaviour and Sanctions policy.

Cyber-bullying incidents are taken extremely seriously and are dealt with in the same way as any other incidence of bullying (see also the Anti-Bullying Policy).

Disciplinary action may be taken where a staff member's use of technology is in breach of the Code of Conduct for Staff (see Faculty Staff Handbook and Business Support Staff Handbook). The staff handbooks for faculty and support staff include more detailed expectations for the appropriate use of technology.

Any concern that an e-safety incident may be an indicator of a child protection issue must be reported to the relevant Child Safeguarding Lead, in line with the Child Protection Policy.

3. Managing Information Technology

3.1 How will our IT system security be maintained?

The school IT systems will be reviewed regularly by the EBT director and the EBT team, with regard to security.

Security strategies will be discussed and agreed between the department of Educational and Business Technology (EBT) and all school departments – security issues will be raised at the Technology Working Group (TWG), for faculty departments and at the COO Meeting for Business Support departments. Urgent or high level concerns will be raised directly with the Management Team.
In the event of a security breach, the EBT director has the authority to take whatever action he/she sees fit in order to minimise the risk to the school, including temporarily shutting down or restricting access to the network.

Security measures will include but are not limited to:

i. All staff members will be required to use strong passwords and to change them regularly.
ii. Separation will be maintained between the guest network and the internal network domains. Virus protection software will be installed on all School PCs and updated regularly.
iii. An internet firewall will be maintained to screen all incoming traffic.
iv. Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail.
v. Files held on the school's network will be regularly checked for appropriate content.
vi. The Network Manager will ensure that the system has the capacity to take the expected traffic caused by internet use.

3.2 How will electronic communication be managed?

Each student in the Junior and Senior Schools has access to their own school-based email account, which is specific to their system login.

Students are able to send e-mails internally and externally for school use, under supervision and/or appropriate guidance.

Student e-mails can be accessed at the request of a subject or class teacher with permission from a member of the Leadership Team of the relevant school.
All staff are issued with a 'tts' email address which should be used for all school related communication. Staff are expected to follow the Email Guidance published by the Communications Team and must take note of the 'principles of responsible use' of ICT included in the staff handbooks.

3.3 How will public access online content be managed?

Personal information of staff, parents or students is collected, used and disclosed in accordance with our Personal Data Protection Policy.

The Public Web site will include the school address, and the e-mail addresses and telephone numbers of: the school offices and the main reception; admissions department; the communications department and the development department.

The Committee for Private Education Singapore (CPE) require faculty staff names and academic qualifications on the public website. These are published alongside staff photographs.

Photographs and video of students will be used on the public website, in online newsletters and on social media in accordance with our current Photo and Video Policy. Students' full names will not be used on public websites when associated with photographs, or in any way which may be to the detriment of students.

The Communications department will take overall editorial responsibility for the public website and the TTS Portal, ensuring that content is accurate and appropriate on all pages directly related to the day-to-day workings of the school.

The school has an official presence on social media. Staff are expected to follow the current Social Media Guidelines issued by the Communications Department when posting on social media, whether using their personal accounts or an official school account.

The copyright of all material published on the public website, online newsletters and social media must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

School managed student blogs will be password protected or run from the school intranet sites.

3.5 How will emergent internet Technologies be managed?

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

4. Cloud Storage

4.1 Benefits of and concerns regarding cloud storage solutions

The School encourages the use of cloud services for file storing and sharing; cloud storage of files can expedite collaboration and sharing of information anytime, anywhere, and with anyone. However, there are a number of information security and data privacy concerns about use of public cloud storage (Microsoft SharePoint, OneDrive, and Google Drive) services at the school. They include:

- The school can no longer guarantee the quality of access controls protecting the data
- The location where the data is stored may not be known
- Using cloud storage client software to synchronise files between work and personal devices could result in sensitive information being held inappropriately on personal equipment.

This policy is designed to maximise the benefits of using cloud storage whilst minimising the risks, by identifying the kind and type of school information that is appropriate for storing and sharing using these services.

4.2 Storage of information - policy for all Tanglin staff members

- The School only supports business oriented cloud storage services such as Google drive and Microsoft OneDrive for business.
- Confidential information, such as personal biodata of staff or students, or other sensitive information (e.g. HR or finance related information) should be maintained in secure systems (e.g. iSams/ Blackbaud) and not stored in cloud based drives.
- Documents that need to be retained long-term, such as templates and policy documents, should be stored on SharePoint or shared network drives, rather than on personal cloud drives (OneDrive, Google Drive etc..).
- Staff are strongly advised to keep more than one copy of important documents.

• Staff should ensure that there is a suitable level of authentication on any mobile or portable device used to download any school related data from cloud storage. Such a device must be password protected.

4.3 Sharing files and folders

Where there is a requirement to share information with others then it is important that individuals who enable the sharing of data do so with the following safeguards:

- Grant access only to the specific folders and files that are required to support the collaboration or information sharing. Ensure that no other folders or files are made available.
- Take care to ensure access is granted to the right individuals.
- Staff sharing information through cloud services have a responsibility to ensure that all collaborators are aware of any privacy or confidentiality issues.
- Remove individuals when they no longer require access to files or folders.

4.4 Synchronising between devices and cloud services

Synchronising information to and from cloud storage is not necessary, however it can provide significant advantages in terms of information availability and speed of access in circumstances where the user will be off-line. Synchronising information across devices requires the following safeguards:

- Devices involved in the synchronisation process must be protected from loss and unauthorised access. Mobile devices must have a “PIN” code or equivalent security enabled.
- Devices involved in the synchronisation process must be protected from malware and kept up to date with operating system security patches.

5. Internet Filtering Policy

Tanglin Trust School has a duty of care to ensure the safety of its community. This applies equally to both the physical and virtual environments. As such the school uses web filtering technologies to prevent access from devices to particular types of internet content.

The filtering technologies aid in the **security and stability of the network** by preventing the download of software that is malicious and / or disruptive or could impact significantly on the performance of the network.

In addition, the filtering technologies **restrict access to material** that is classified by the Leadership Team as **objectionable or inappropriate**.

All users are reminded that the web filtering policy is not a total guarantee of web safety and is complemented by the appropriate responsible use agreement and on-going education in digital citizenship.

5.1 Current Filtering Guidelines

At present the Leadership Team of Tanglin Trust School has agreed to the following guidelines.

a. Where possible enforce Safe Search in web search engines.
b. Restrict access to websites that fall under the following categories (as defined by the filtering software)

• Abortion • Adult mature / content • Alternative spirituality / belief • Chat / IM / SMS • Child pornography • Controlled substances • Extreme • Gambling • Games • Hacking	• Humour / jokes • Intimate apparel / swimwear • Malicious websites • Marijuana • Nudity • Peer to peer • Personal / dating • Phishing • Piracy / copyright concerns • Pornography • Proxy avoidance	• Scam / questionable / illegal • Sex education • Sexual expression • Social networking • Spam • Suspicious • Violence / hate / racism • Weapons

5.2 Filtering Order

It is not uncommon for a site to be classified under more than 1 category by the internet filters. In such instances the logic of the internet filters is to apply the more restrictive policy first.

For example, if a site was classified as “games” and also “education”, the site would be blocked by the “games” rule as that is applied before the “allow education sites” rule.

5.3 Process for allowing / blocking access to an individual site.

If a teacher requires an individual site to be blocked or unblocked for legitimate educational purposes, then they should submit an e-mail to EBT Help Desk requesting access and a very brief overview of the reasoning. This is for record keeping purposes only; a log of the requests will be available for the Leadership Teams of each school to review.

Such examples have included access to certain alcohol and sex education websites for the purpose of PSHCE lessons.

Staff should be aware that intentionally attempting to circumvent our filtering policy could expose the network to security risks and will be treated as a breach of the Code of Conduct.

5.4 Process for review of the categories or policy.

Tanglin Trust School will continually review the categories and may implement different filtering policies for different year groups where appropriate.

If a staff member wishes to have the categories or policy reviewed, they should first approach the Leadership Team of their individual school.

If the Leadership Team of the school concerned approves the request, it would then be submitted to the Director EBT to be implemented, subject to any technical issues.

If there is a technical issue that prevents immediate implementation, for example if EBT is concerned over the security of the network, or if there are implications for the other schools, options would be investigated for discussion.

Any change that will affect the whole school must be discussed by the TWG and approved by the whole school Leadership Team.

6. Communication of this Policy

6.1 How will e-safety be introduced to students?

Awareness of E-safety and the importance of safe and responsible internet use are taught explicitly, through Tanglin's PSHCE and Computing curricula. This planned curriculum aims to introduce issues and strategies for staying safe at an age appropriate level and bearing in mind the increasing access to technology as students progress through the school. The curriculum materials are reviewed regularly and draw on available expert advice, particularly from commonsense media (https://www.commonsensemedia.org/educators)

The Responsible Use Guidelines (Appendix 1), including Internet safety advice, are incorporated into the Code of Conduct for Students and are prominently displayed around the school. For Senior and Junior students, the Responsible Use Guidelines will also be available on the school's intranet sites (TTSPortal; Firefly).

Students will be informed that internet use is monitored and logged and that these logs can be retrieved under the direction of a Head of Year or member of Senior Management Team.

Instruction in responsible and safe use will precede internet access.

6.2 How will the policy be discussed with staff?

All staff will be made aware of the School Technology and E-Safety Policy and its application and importance explained.

Staff should be aware that internet traffic can be monitored and traced to the individual user.

Staff should be aware that school e-mail can be retrieved and opened under the written direction of the relevant Head of School or CEO; discretion and professional conduct is essential.

6.3 How will parents' support be enlisted?

Parents' attention will be drawn to the School Technology and E-Safety Policy in newsletters, the school brochure and on the school website.

E-safety related incidents will be handled sensitively to inform parents without causing undue alarm.

A partnership approach with parents will be encouraged. This will include parent information sessions and newsletter articles to explain how technology is being used in school and suggestions for safe internet use at home.

7. Role of Governors

7.1 The role of the Education Sub-Committee of the Board of Governors (ESC)

The role of the ESC is to be aware of the School's approach to E-Safety and of how this 'Technology and E-Safety' policy relates to more general policies on behaviour and child protection, as well as the PSHCE (Personal, Social, Health and Citizenship Education) curriculum.

Any changes to this policy must be approved by the ESC.

Appendix 1 – Responsible Use Guidelines

Infant School

Responsible Use Guidelines:

- I will not tell other people my ICT passwords (except for trusted adults).
- I will not give out my personal details such as my name, phone number, birthday or home address.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will only use ICT in school to help with my learning.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- If I accidentally find anything that worries me I will click on Hector and then tell a trusted grown up immediately.
- I know that my use of ICT can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my e-Safety.

.

Prepared By	Approved By	Reviewed & Revised	Reviewed By
TWG (Technology Working Group)	ESC – Feb 2012 ESC – Nov 2017	Sep 2014; Feb 2015 **June 2017**	TWG

Junior School

Responsible Use Guidelines:
Principled - Caring - Communicators

- I will only use ICT in school for school purposes
- I will protect my identity, and that of others, by not sharing personal information online such as names, phone numbers, addresses, passwords or the name of the school
- I know that my use of ICT can be checked and that my parent/carer will be contacted if a member of school staff is concerned about my e-Safety
- I will only open/delete my own files
- I will only use my school e-mail address for school related activities
- I will only open e-mail attachments from people I know, or whom my teacher has approved
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- If I accidentally find anything inappropriate whilst online I will tell my teacher immediately
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community

iPad Usage:

- I understand that use of iPads in lessons is at the choice of each teacher
- I will protect my identity, and that of others, by not sharing personal information online such as names, phone numbers, addresses, passwords or the name of the school
- My use of technology and online tools will be responsible and respectful
- I will not record or publish audio or video of myself or any member of the community unless instructed to do so by a teacher.

Senior School
Technology for Learning
Responsible Use Policy

Principled - Caring - Communicators

- I will use technology and online tools **responsibly and respectfully**

- I will protect my identity, and that of others, by not sharing **personal** information online such as names, phone numbers, addresses, passwords or the name of the school

- I will only record, upload or distribute **audio, images** or **video** of myself or any member of the community with the agreement of the people involved and when instructed to do so by a teacher as part of a learning task

- I will only look for, create, contribute to, save or distribute **appropriate** material and will report anything inappropriate that I find to my Head of Year

- I will be a **principled** learner when using online resources and will always credit other people's work

- I will respect the school server and wireless network **settings** and **filters**

- I may wear **headphones** when doing private study or when directed by a teacher, but not when moving around the school site

- I will keep my **mobile phone** on silent mode and out of sight during **school hours*** unless instructed to use it by a teacher as part of a learning task

- I understand that my **use of technology** is monitored and that a breach of this policy will result in sanctions, in line with the Senior School **student code of conduct**

- ***School hours** means from my arrival on the school site to the end of my last lesson

Personal Device usage in Key Stage 3 and 4

- I will bring my personal device fully charged to lessons, in an approved case, along with pocketable earphones
- I will use my personal device in lesson time at the discretion of the teacher
- I may use my personal device at break, lunch and after school hours in **the library**

Prepared By	Approved By	Reviewed & Revised	Reviewed By	Next Review
TWG (Technology Working Group)	ESC – Feb 2012 ESC – Nov 2017	Sep 2014; Feb 2015 **June 2017**	TWG	Jun 2019