The Sheffield Private School

E-Safety Policy

1 Purpose

The Sheffield Private School (TSPS) recognises that the internet and other technologies provide extensive opportunities for children and young people to learn. The purpose of internet use in school is to raise educational standards, to promote pupil achievement and well-being, to support the professional work of staff and to enhance the school's management information and business administration systems.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet access is an entitlement for students who show a responsible and appropriate approach to its use. The internet is an essential element in education, business and social interaction. TSPS has a duty to provide students with quality internet access as part of their learning experience. TSPS is committed to ensuring that all its students use existing and up and coming technologies safely.

2 Scope

The school will introduce the procedure to students. A module on responsible internet use and e-safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately. Instruction on responsible and safe use should precede internet access.

3 Role and Responsibilities for Students' E-safety

3.1 The School will:

- Address the topic of E-safety, including cyber bullying, during ICT lessons;
- Students will learn appropriate internet use and be given clear guidance for internet use. Staff should guide students in online activities that will support the learning outcomes planned for the students' age and maturity;
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and copyright law;
- Help students learn to evaluate internet content. Specific lessons will be included within the ICT Scheme of Learning that teaches all students how to read for information from web resources. Students will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work;
- Enforce online communications, social networking and mobile technology school rules;
- The use of online chat and social networking sites is not permitted in school;
- Students are not permitted to bring mobile phones to school;
- The consequences of inappropriate use of the internet, or mobile phones, will be clear to students.

3.2 The School Leadership Team will:

- Provide curriculum about appropriate etiquette for online behaviour, including awareness about interactions and communication with others on social networking websites and in chat rooms;
- Organise focused workshops on raising awareness of cyber bullying and appropriate responses in dealing with it;
- Ensure safety and security of students when using internet and electronic communications;
- Provide students, staff and parents with guidelines and instructions for student safety while using the Internet.

3.3 Students will:

- Ensure they do not divulge any information about themselves or other persons on social media or through any other form of electronic communications over the Internet;
- Not disclose their home address or telephone numbers;
- Never upload any images of themselves or others without permission of parents or staff;
- Not Plan or arrange appointments with anyone they have met on the Internet;
- Take proper measures if they receive any message that is inappropriate or makes them feel uncomfortable. They should immediately inform an adult they trust;
- Ensure they are not exposed to information or images that might harm them or cause them discomfort;
- Speak out against cyber bullying and immediately get in touch with the relevant staff or parents;
- Avoid trying to access websites that have adult content and are restricted;
- Not damage computers, computer systems, software, or computer networks;
- Respect themselves and all other users through good network etiquette;
- Say no to plagiarism and give due credit to anyone whose work they are using for educational purposes;
- Help in raising awareness across school of acceptable and smart use of the Internet.

3.4 Staff will:

- Educate students about appropriate and safe internet usage, including interaction and communication with other people on social networking websites and in chat rooms;
- Encourage awareness about cyber bullying and give clear guidelines as to the steps that are to be taken and people that can be approached;
- Monitor and ensure that there is no misuse of the Internet;
- Raise awareness about the advantages and disadvantages of using Social media like Facebook, Twitter, YouTube, Google+, and Flickr;
- Use the online web-based interactive communication technologies to enhance students' education and learning and to facilitate collaborative study habits in students;
- Improve peer collaboration and sharing of internet resources through sustained usage of online web-based interactive communication;
- Empower students with 21st century learning tools to enable them to become independent learners;
- Share outstanding teaching practises through electronic communication;
- Develop cross country collaboration in students encouraging knowledge and skill based projects;
- Incorporate ICT in all areas of the curriculum to encourage the holistic approach of the students;

- Develop the presentation skills using ICT for project work and competitions.

3.5 Parents will:

- Monitor and enforce their own family values to their children making them aware of the importance of using the Internet safely;
- Involve their children in regular discussions regarding the different challenges that are presented through the Internet;
- Ensure that the children are aware of the acceptable internet discipline and the consequences if the rules are broken;
- Maintain clarity and consistency on what is permissible and what activities are unacceptable;
- Assume complete responsibility for monitoring their children's use of internet at home and outside school.
- Have complete awareness of cyber bullying and ensure that the children are not being subjected to it in any form through monitoring and discussions;
- Inform and work with the school if any misuse is reported or found;
- Seek help and support from the school in case of any incident that involves cyber bullying;
- Be well informed about the work or projects given to the children to rule out any misuse. In case of any concerns check with the school immediately.
- Ensure that age appropriate restrictions are in place on student devices that prevent their child accessing age-inappropriate material.
- Regularly monitor their child's online activity to ensure that their child is behaving responsibly and safely while online.

4 Procedures for dealing with Cyber Bullying

This is outlined in connection to the Behaviour Policy at TSPS. The initial stage of any identified process of cyber bullying will be investigated and reported as stage 1. Should the incident be proven as sustained bullying of other students then it will be reported as Stage 3. This will involve Pastoral Support Plan and a Final Warning.

5 Managing Filters

TSPS can permit or deny sites that they feel inappropriate for the duration they choose using the server access system. If staff or students discover unsuitable sites, the URL (address) and content must be reported to the IT technicians.

To ensure appropriate network filters, students will only use the designated BYOD or the TSPS student wireless connection in school and will not attempt to bypass the network restrictions by using 3G or 4G networks or a VPN. Non-compliance will result in loss of the ability to bring personal devices to school for a period to be determined by the school

Processing or accessing information on school property related to "hacking," altering, or bypassing network security policies is in violation of the BYOD guidelines and will result in disciplinary actions. Students can only access files on the computer or internet sites which are deemed relevant to the classroom curriculum and suggested by the subject teacher

6 Assessing Risks

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for students. The school will take all reasonable

precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. TSPS cannot, therefore, accept liability for the material accessed, or any consequences of internet access.

7 Managing Website Content

The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
Parents will be given the opportunity to say if they are not happy for their child's photograph to be published.

8 Informing Parents

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

Students and parents participating in BYOD must adhere to the Student Code of Conduct, as well as BYOD guidelines of TSPS.

9 Informing Staff of their Roles and Responsibilities with Regard to E-Safety

- All staff, including teachers, classroom assistants and support staff, will be provided with the School E-Safety Policy and its importance explained.
- The school's consequences for internet and mobile phone misuse are in line with the schools behaviour management policy, removal of internet and email as a form of sanctioning will only be done as a last resort and only after consultation with all parties concerned.
- All staff must accept the terms of the 'Responsible Internet Use' statement before using any internet resource in school.
- Any complaint about staff misuse must be referred to the Principal.

10 Network folder usage

The school will issue each student a network folder, which is part of the schools network administered by the schools technology team. The purpose of this folder is for the convenient storage off personal data.
It is envisioned that students will store records relating to their studies. It's hoped that students will make increasing use of their network folders as the year progresses, saving copies of all of their work and assignments throughout the year, in order develop an electronic portfolio.

The home folder is the personal property of the person who is given access to it unless needed, no-one will access an individual's personal network folder, however, should the need arise, access can be gained by school administrators.

Misuse of one's network folder is a serious matter and will be referred with the behaviour policy at TSPS

Misuse can be generally defined as, but not limited to:
Storing offensive material or material of culturally/politically insensitive nature.
Knowingly storing data that is illegal in the UAE.
Knowingly storing viruses, Trojans, or any other data that may damage the network.
Attempting to hack into another person's network file.

Deleting other user's data from the shared network drive.

Appendix to the E-Safety Policy

Email Acceptable Use Policy

This Email Acceptable Use Policy applies to all TSPS students, visiting students and to those using TSPS's ICT Network.

General Principles

- TSPS e-mail accounts are primarily to be used for educational purposes. However, some limited personal use is considered acceptable.
- Any information distributed through the school network may be subject to scrutiny.
- E-mail user accounts may be accessed by the school as part of an authorised investigation.
- The use of computing resources is subject to UAE law and any illegal use will be dealt with appropriately. For example the Police can have a right of access to recorded data in pursuit of an investigation.

Guidelines:
It is unacceptable to:

- Send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Represent personal opinions as those of TSPS.
- Reveal or publicise confidential or proprietary information which includes, but is not limited to financial information, databases and the information contained therein, computer network access codes, student/staff information and business relationships.

Review: September 2020

Next Review: August 2021