Online Safety and Acceptable Use Procedures

Person(s) responsible for this policy		Second Master, Head of Digital Learning	
Last review by	**G Cross**	**Review date**	**September 2019**
Date of next review		**September 2020**	

The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the curriculum and a necessary tool for staff and pupils.

At SCHS**,** we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. Everybody in the school has a shared responsibility to secure any sensitive information used in their day-to-day professional duties.

This document details the school's procedures relating to e-safety and should be read in conjunction with the e-safety policy and acceptable use agreements for pupils and staff. It is inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, and other mobile devices).

1. Teaching and learning – Pupils and the Web

1.1 Internet use

- All electronic traffic on the school network is monitored and logged using Fortinet.
- The GDST will maintain and update a central filtering policy; the school's ICT operations manager, Second Master, Head of Prep. School, and Head of Digital learning will review the central policy, amending as needed to ensure it is appropriate for the different phases of the school and reflects current trends and developments.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use through ICT lessons, PSHCE lessons, year-group and whole-school assemblies. This will also cover the online risks that they may encounter outside school.
- Research techniques, including the skills of knowledge location, retrieval and evaluation using the internet will be taught by subject teachers and the school librarian. This will include

making pupils critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Pupils are taught about copyright, data protection, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities in the ICT curriculum.
- Through PSHCE, ICT lessons, form time and informal discussions, pupils will be made aware of the impact of cyber bullying and know how to seek help if any form of online bullying affects them.
- The acceptable use policy is discussed with pupils are the start of the academic year in ICT lessons
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- Staff will preview any recommended sites before use

The schemes of work for ICT and PSHCE will contain more detailed information on when it is taught and what is covered.

2. Managing Internet access using school-based systems

2.1 Information system security

- The ICT Operations Manager in conjunction with the SLT and Trust ICT team will review the security and robustness of school-based systems regularly.
- Access to the school network is only possible by a valid user name and password. Password strength is enforced using the active directory.
- All school owned computers have virus protection installed, which is kept up-to-date.
- Before any staff or pupil owned device is connected to the guest network, the ICT team will verify that appropriate anti-virus software is installed.
- Any external devices including portable hard drives and USB drives used by staff will be encrypted when they are connected to any school computer.
- The local ICT team will work with the GDST ICT team to review and implement appropriate security procedures to protect users and data. These will be discussed at termly GDST technical days.

2.2 Managing filtering

- The DSL and Second Master will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Weekly reports will be reviewed by the aforementioned staff to look for child protection concerns and any general patterns.
- Through ICT lessons and PSHCE lessons, pupils will be instructed to report unsuitable sites to the e-safety Co-ordinator or their own teacher. The e-safety co-ordinator will investigate the site and, if necessary, liaise with network staff to ensure the site is blocked.

2.3 Email and messaging

- When using the school computers, pupils may only use school email accounts for communication and registering for online resources.
- Staff will use accounts provided by the school for all work-related and professional duties.

- All communication via the school networks, both wired and wireless, will be filtered and monitored using Fortinet.
- ICT teachers will remind pupils of how the acceptable use agreement and e-safety relate to internet-based communications. This will include not revealing personal details about themselves or others in email communication, arranging to meet anyone without specific permission, and never to send hurtful or damaging messages to anyone

2.4 Managing emerging technologies

- The ICT steering group meets termly and will review the educational benefits of emerging technologies, assessing the associated risks. This group will make recommendations to SLT before implementation.
- Departmental digital champions will work with the Head of Digital Learning to reassess the suitability of technology and systems over time and check that they remain suitable, secure, and effective.

3 Published content and Pupils

3.1 The school website

The Head Master will take overall editorial responsibility and ensure that content is accurate and appropriate. The Marketing department and ICT team support him in this role, reviewing the content of the website regularly to ensure data protection and safeguarding procedures are followed. Any external agencies that are engaged to photograph or film on school property or at an external school event will be subject to appropriate checks before commencing work and appropriate supervision by school staff.

3.2 Publishing pupils' images and work on the web

Open/public sites

- Pupils' full names will not normally be used on the website, particularly in association with photographs and locations of events such as forthcoming sporting fixtures.
- The Marketing department will select photographs for publication on the website, or elsewhere, and these will be approved by the Head Master.
- Care will be taken when taking digital/video images that pupils are appropriately dressed and that permission has been given by parents/guardians for their daughters to be photographed/filmed.

Closed/ Secure sites

The school provides access to secure communications via SchoolPost and Agora. These systems are secured by personal logins that are unique to each parent, providing access to personal mailboxes. When a pupil leaves the school the Registrar and Finance Officer automatically disables access to these systems.

3.3 Social networking and personal publishing

- Access to social network and chat sites is blocked using the school's filtering system. Any requests for access will be reviewed by the Second Master and discussed with SLT or other relevant groups before access is enabled for individuals/groups either for a period of time or permanently. Access will be monitored if it is granted and its continued use reviewed on a regular basis.

- Website creation is taught as part of the Lower Fourth ICT curriculum. Pupils are reminded of the acceptable use agreement before this unit of work commences and the importance of not sharing any personal data during this unit of work. Websites created in this unit of work are not published to the internet.

3.4 Using web sites with pupils

In a rapidly changing electronic world it is impossible to ask permission from parents for every new site that might be used with pupils or that pupils might discover for themselves. Instead the school will abide by the following principles:

- All sites are filtered via the GDST system to minimise the risk of inappropriate material being accessed.
- All internet traffic is monitored and logged
- If pupils are asked to make online accounts for access to materials, identifiable personal information will not be disclosed and only school emails will be used.
- Staff will review sites before they are first used to ascertain whether they are relevant and safe.
- The selection of sites will be altered to reflect the ages and abilities of the pupils.
- Staff will make the ICT team and e-safety coordinator aware of any concerns that arise when pupils are accessing websites.

4. General provisions of the policy – Staff & Pupils

4.1 Protecting personal data

- Any recording, processing, or transfer of personal data will be carried out in accordance with the Data Protection Act 2018.
- All school computers are encrypted and any external devices used by staff are encrypted when connected to a school computer.
- Access to SIMS is restricted to authorised personal with user names and passwords. User-level permissions further restrict access to any personal information stored in the electronic system.

4.2 Authorising internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement for Staff' on commencement of employment and before using any school ICT resource.
- All pupils will be introduced to the 'Acceptable ICT Use Agreement for Pupils' and the reasons for the rules will be explained to them in ICT lessons.
- When any computer user accesses the school system for the first time they will be prompted to read the Acceptable ICT Use Agreement and give electronic consent that they agree to abide by its terms and conditions. The responses are stored electronically and can be reviewed by the local ICT team and GDST ICT team.
- The Head Master's PA will keep any paper copies of signed agreements in staff personnel files.

4.3 Staff use of Equipment and the Internet

Expectations are set out in the Acceptable Use Agreement for staff mentioned above. Any breach of this agreement is grounds for disciplinary action in accordance with GDST procedures. Staff will be

informed of any allegations and a member of the school's SLT will investigate them in accordance with the GDST policy.

4.4 Assessing risks

- SLT will review the e-safety procedures and policy periodically considering any changes to the curriculum or ICT provision at the school. GDST personnel including the ICT team, Education team, and Legal team will be consulted as appropriate.
- Display Screen Equipment (Health and Safety) assessments are completed by a member of the administrative team for any member of staff who uses ICT equipment for long periods of time when they commence employment, or if their usage pattern changes.
- The school will help pupils develop safe working practices when using Display Screen Equipment through ICT lessons. In particular adjustable seats are provided at pupil workstations, the ICT team will monitor and adjust the setup of equipment in computer rooms, and any refurbishment work or new developments will take account of appropriate layout of any ICT facilities.

4.5 Handling e-safety complaints

- Complaints about ICT misuse by pupils will be dealt with by a senior member of staff under the disciplinary procedures of the school and according to the nature of the complaint.
- Any complaint about staff misuse must be referred to the Head Master/senior manager and will be investigated. Depending on the outcome of the investigation action may be taken in accordance with GDST disciplinary procedures.
- Complaints of a child protection nature must be dealt with in accordance with statutory child protection procedures.
- The school's complaints procedure and the policy will be published on the school's website.

5. Safe Use of Images and mobile devices

5.1 Taking of images and video

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Head Master, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others outside of lessons. In lessons permission must be sought from the class teacher and relevant to the lesson plan. Any content must be stored on the school network and not published externally.
- The school allows staff to bring in mobile phones for their own personal use. However, they should not normally be used in the classrooms, toilets, changing rooms or in other areas where there are pupils during the school day.
- Pupils and staff must have permission from the Head Master before any image can be uploaded for publication.

5.2 Storage of images/videos

- All images of pupils and staff will be stored on the school network in photo archive

- Access to the photo archive is restricted to school staff with valid logins and can only be accessed when in school or on the GDST internal network.
- The local ICT team and Marketing department will be responsible for maintaining the photo archive

5.3 Webcams and video-conferencing

- If a specific learning activity requires the use of a webcam/video-conferencing facility and pupils will be filmed then consent will be sought from the Head Master, and the parents of all pupils involved.
- The video stream will not be recorded or stored in a digital retrieval system
- Pupils will be supervised at all times.

5.4 Mobile phones

- Personal phones will not be used to contact pupils or parents.
- The school will provide school approved devices for use on school trips or for senior members of staff.
- In the event of an emergency, a personal mobile phone can be used to contact the emergency services and to communicate with the school. Further guidelines are provided in the educational visits policy.

6. Communicating the policy

6.1 Introducing the e-Safety Policy to Children

- ICT teachers will review the acceptable use agreement with pupils in lessons
- E-safety is the focus of a whole school assembly each year.

6.2 Staff and the e-Safety Policy

- All staff will be given a copy of the e-Safety Policy at the start of the academic year during safeguarding training by the safeguarding lead. Staff will be made aware that internet traffic can be monitored and traced to the individual user.
- All staff will be given a copy of the school's code of conduct at the start of the academic year
- They will be required to sign to indicate they have received these documents.

6.3 Enlisting parents' support

- Parents/guardians will be sent a copy of the acceptable use agreements and e-safety policy via SchoolPost and asked to sign the agreement in the pupil planner. In the Prep. school parents sign and return a hard copy of the agreement.
- All parents are invited to an e-safety evening

Appendix: Teaching of e-safety in the curriculum

Year 1	Keeping personal information safe
Year 2	What to do and where to go for support about concerns when researching on the internet
Year 3	Using technology safely
	Safely using email and video conferencing
Year 4	Using a range of ways to report concerns when working online
	Wiki aware: how anyone can publish any content online
Year 5	Creating an e-safety poster
	Blogs: how anyone can post on a blog site
Year 6	Mobile phone safe use
Upper Third	Creating strong passwords and security of usernames
	e-safety leaflet
	Cyber bullying
	Hackers/Viruses/Malware
	Chat rooms
	Phishing/Spam
Lower Fourth	Publishing content to the web and personal information