Learning Together to make a Positive Difference

Staple Hill Primary School
E-Safety Policy 2018

Introduction

- This document is a statement of the aims, principles and strategies for e-Safety at Staple Hill Primary School.
- It must be read in conjunction with:
  - Safeguarding Policy Incorporating Child Protection
- It will clarify the legal requirements and responsibilities of the school
- It will reinforce and safeguard the safety of pupils and others who use the school
- It will clarify the school's approach to e-Safety for all staff, pupils, governors, parents/carers, external agencies and the wider community
- It was developed through a process of consultation between the ICT Leader and staff

Rationale

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience. Pupils use the internet widely outside school and will need to learn how to evaluate internet information and take care of their personal safety and security. The purpose of internet access in school is to:

- raise educational standards,
- support the professional work of staff
- enhance the school's management information and business administration systems.

Access to the internet is a necessary tool for staff and pupils. It is an entitlement for pupils who show a responsible and mature approach.

Teaching and Learning

- Teachers, parents and pupils need to develop good practice in using the internet as a tool for teaching and learning. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils and agreed levels of staff supervision.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Although in school the pupils are unlikely to access inappropriate material or be in contacts with outside users, it is important that they develop an awareness and

understanding of the possible risks and the importance of personal safety in other environments. Whole school protocols will be established to deal with any inappropriate content or networking that might emerge. Incidents will be reported directly to the local authority in order to block any websites deemed inappropriate.

- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.
- In accordance with the Child Protection Policy, pupils will be taught about 'Stranger-Danger' in relation to the internet and on-line chat rooms.
- https://swiggle.org.uk/ will be used as the home page in school to encourage safer searching.

Managing Internet Access Information system security

School ICT systems security will be reviewed regularly. Virus protection will be updated regularly. Security strategies will be discussed with the Local Authority.

E-mail

Pupils may only use approved internal e-mail accounts on the school system. Pupils will only use the email accounts under supervision. Currently, there is no access to pupil emails.

Published content and the school website

Staff or pupil personal contact information will not generally be published. The contact details given online should be held confidentially, in the school office. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Parents/Carers will be asked to complete permission slips for the publication of any still or moving images of their children on our school website/Twitter/Local Media, on first entry to the school. Only those with permission will be used and further permission will be sought to use images in external publications e.g. local media newspapers, National competitions, etc where original permission is declined (only if necessary). Full names will never accompany these photographs. Staff will ensure that they are aware of every pupil in their class who does not have permission for images to be used. They will be responsible for only submitting appropriate images excluding these pupils for inclusion on our school website/Twitter/Local Media. Only agreed staff will be allowed to publish images to Twitter (Headteacher & SBM).

Parents/Carers will be clearly informed of the school policy on image-taking and publishing especially with regard to:

- Safeguarding pupils during school events i.e. photography and video will not be allowed at any performances to Parents/Carers. Parents/Carers will only be allowed to take still images of their own children at the end of a performance, if they wish.
- Publication of images on the school website/Twitter
- Publishing of images in any other external publication e.g. newspapers, etc.

Social networking and personal publishing

- Pupils do not have access to social networking sites in school but are educated in their safe use.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. This includes the use of profile pictures while dressed in their school uniform.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use appropriate nicknames and avatars when using social networking sites.

Managing filtering

- The school will work with South Gloucestershire LA, SWGfL and Becta to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable online materials, the site must be reported directly to the Local Authority and Downend IT Team.
- The Local Authority and Downend IT Team, as appropriate, will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. All staff are expected to have their mobile phones locked away during the day. These will only be used, if necessary, during their break times. Pupils are not allowed to bring mobile devices to school including mobile phone, Smart Watch or iPad, etc. If staff discover such devices with pupils, they will be confiscated and taken to the Administration Office for safe-keeping. Parents/Carers will be notified of the discovery and the device will be returned to the pupil or Parent/Carer at the end of the day.
- As part of our E-Safety curriculum, staff frequently remind pupils that the sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden. Any instances of this behaviour that is reported to us will be passed on to

the appropriate Parent/Carer. Pupils will be spoken to as an individual, group, class or year group, as appropriate to the circumstances that arise.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of internet access but we will have established a clear protocol for reporting inappropriate material.

The school will audit ICT use regularly to establish if the E-safety policy is adequate and that the implementation of this is appropriate and effective.

Handling E-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints linked to safeguarding of pupils MUST be dealt with in accordance with the school's child protection procedures.
- Pupils and Parents/Carers will be informed of consequences for pupils misusing the internet.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communications Policy

Introducing the E-safety policy to pupils

- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- Regular training for staff in E-Safety will take place as part of the development of the Computing Curriculum. Links will be made with the Personal Social and Health Education (PSHE) curriculum.
- The E-Safety Agreement will form part of every child's published planner which will be used daily at home and in school.

Staff and the E-Safety policy

- All staff will be given the School E-Safety Policy and its importance explained. They will ensure that all guidance is upheld and will read this policy in conjunction with the 'ICT Policy' and the 'ICT Staff Acceptable Use Policy' in addition to associated agreements relating to the use of school iPads and laptops.
- Staff must be informed that network and internet traffic can be monitored and traced to the individual user.
- Staff will always use a child-friendly safe search engine when accessing the web with pupils.
- Staff will follow agreed protocols for dealing with emerging inappropriate internet content.

Home-School Link

- Internet use in pupils' homes is increasing rapidly. Unless Parents/Carers are aware of the dangers, pupils may have unrestricted access to the Internet.
- Parents' and Carers' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school website.
- The school will maintain a list of E-safety resources for Parents/Carers which will be published on our school website.
- The school will ask all new Parents/Carers and pupils to sign our 'E-Safety Agreement' now featured in each child's planner. These agreements will be revisited during their child's time in our school and are to be signed again at the beginning of each academic year.

Date	Notes
24 November 2016	Ratified by FGB
19th November 2017	Reviewed and updated by Arwa Said
20th November 2017	Reviewed by S & C Committee
	Ratified by FGB
15th October 2018	Reviewed by S & C Committee
	Ratified by FGB