Southfields Primary School

Internet Safety Policy

Date agreed: September 2022
Review Date: September 2024

This policy, having been presented to, and agreed upon by the whole staff and Governors, will be distributed to:

- All teaching staff
- School governors

A copy of the policy will also be available in:

- The Staffroom
- The Head's office
- School web site

This will ensure that the policy is readily available to visiting teachers, support staff and parents.

Southfields Primary is totally committed to social justice and improving life chances for potentially vulnerable children. It is dedicated to sharing its work and findings beyond the school to improve outcomes for as many children as it can reach and has a particular specialism in Speech and Language development.

1. Purpose of the Document

The internet is becoming as commonplace as TV and telephones and as teachers it is key that we teach children how to safely develop their use of this essential life skill. This document will explain, specifically, the threats posed by the Internet and its use in a school environment and how teaching staff, pupils and the school body as a whole will minimise these and work safely when using this vital tool. This document is in addition to our Internet (Acceptable Use) Policy.

(The use of mobile phones is not permitted in school time, children are not permitted to bring them to school). For more guidance on the use of personal mobile devices, please refer to our 'Bring Your Own Device' Policy.

2. Core Principles of Internet Safety

- Guided Educational Use – The internet can provide many educational benefits to children including access to information from around the world. Use should be planned, task – orientated and educational within a regulated and managed environment.
- Risk Assessment – Schools need to ensure that they are aware of the risks and pupils and teachers need to know what to do when they come across inappropriate material.
- Responsibility – Internet safety depends on staff, schools, governors, advisers, parents and in some cases in KS2 the pupils themselves taking responsibility for the use of the Internet.
- Regulation – The fact that this resource is ever growing and multi – faceted means its use will undoubtedly attract regulations for its use. The use of some features will be banned, for others fair rules, clearly displayed and explained will help all users make responsible use of this resource.
- Strategies – The document will address these issues and help to ensure that children are safe whilst using the Internet. The key features will be limiting use, supervision and developing the responsibility in children to be vigilant, sensible and to become positive digital citizens and their own gatekeepers.
- Data Protection – in line with planned changes to Data Protection Regulations all staff, governors, schools, advisers, pupils and parents have a responsibility to protect the data they own or have access to.

3. How does the Internet Specifically Benefit Education?

The Government has set targets for broadband Internet use in all schools. This target has been driven by the following benefits to children and staff alike is detailed as follows:

- access to worldwide educational resources
- inclusion in Government initiatives
- access to experts in many fields
- Staff professional development through national campaigns, good practice and educational materials.
- Communication with support services and colleagues
- Improved access to technical support.
- Exchange of curriculum and administration date with LA and DfES.
- Sharing work via social networking such as Twitter (see Social Networking Policy) and our School Blog (see separate rules), which supports the New Curriculum Points of Study.

4. How will the risks posed by Internet use be assessed?

The school will take all reasonable precautions to ensure that users access only appropriate material. Due to the international scale and linked nature of the Internet content is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Peterborough Local Authority can accept liability for the material accessed, or any consequences of Internet access.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

5. How will the policy be introduced to pupils?

The school will:

- Operate the "Firewall" filtering system recommended by Peterborough Local Authority
- Seek authorisation from parents. Any issues that parents have with the system must be drawn to the attention of the school.
- Brief and explain the risks to children
- Ensure the children are aware of how to react in the event of finding unsuitable features on the Internet
- Supervise children when using the Internet.
- Teachers will share in the responsibility for the safety of children online and be vigilant of internet activity which causes concern. Teachers will log any concerns regarding the welfare and safety of children online using the 'Logging Concerns' proforma.
- Attach notices encouraging vigilance to all internet linked computers used by the children. KS1 and KS2 will be different.
- Have rules for KS1 and KS2, showing pupils how to be a good Digital Citizen.
- Children will be taught how to stay safe online through regular E-Safety lessons

6. How will the Internet Enhance Learning?

- Every term children will review Internet Safety websites, (age appropriate,) and will teach age appropriate e-safety lessons. Teachers will plan this into their medium term plans for ICT.
    - Hector Protector is used as a screen cover so that anything accidentally accessed can be covered whilst an adult is informed.
    - CEOP (Child Exploitation and On-line Protection Centre) training for secondary children and young people (and Year 6 Primary children) is annual and part of the PSHE curriculum for raising awareness on staying safe and being responsible for both teachers and pupils. A link to the www.thinkukknow.co.uk website is part of the skin layout for further advice and information on children's or young people's personal on-line spaces.
- Access to the Internet will be limited. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils.
- Internet access will be planned to enrich and extend Learning activities.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned
- Pupils will be educated in effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- Emerging technologies will be assessed and evaluated by the Headteacher and the Computing coordinator. Their educational benefits and risks will be investigated before use in school is allowed.

7. How will pupils learn to evaluate Internet Content?

Throughout life children develop the skill of selecting and evaluating the quality and appropriateness of all information they are subject to online. It is our responsibility to encourage children to become critical thinkers when online. Through supervision children need to be taught to explore and when they come across inappropriate or misleading material to report it to the adult in charge. Children should be given other sources of information including visits, books, audio tapes and videos to back up the information found on the Internet.

If children or staff gain access to or discover unsavoury sites, then they should:

- note the URL, (www or http// address)
- report this to the Staff in charge and the ICT Technician/Support.
- This will then be reported to the LA ICT coordinator as this is a breach of the safety facilities put in place.

8. How will Email be managed?

Pupils will not have access to Email of their own in school.
They will all be informed forcefully that they will not reveal their login details for ICT learning aids (such as BugClub, Mathletics) to others.
For lessons on the email as a system they will use the group system which will be monitored and managed by the teacher.

Teachers will use email as a form of communication within the school body and externally. They will all have a school email address to be accessed both in school and outside. Teachers must not use their personal email address for school related communications (see BYOD for further information). Chat sites are not to be accessed via the school system. This is in line with the planned changes to the Data Protection Regulations.

9. The school Website, Blog and Twitter

The above will be administered and owned by key members of staff at Southfields, who will ensure that:

- The contact details are up to date at all time. Contact information should be the school address, school email and telephone number. There should be no private numbers or home information.
- Teachers are responsible for uploading true information and facts onto their part of the website, blog, Class Dojo and Twitter page. Our tweets are in public view and so it is the responsibility of all staff and parents/carers of children attending Southfields to ensure that tweets are in line with our Social Networking Policy.
- Teachers must ensure that no copyright laws are being broken when they upload information.
- Website content should be reviewed every 6 months by the section owners and content updated accordingly. The review should be focussed on accuracy and appropriateness.

- Twitter and Blog content should be reviewed monthly by the section owners and content updated accordingly. The review should be focussed on accuracy and appropriateness. Only children whom have signed the Acceptable Use Agreement for the Blog will be able to contribute to it – teachers will frequently review the Blog.
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupil names must not appear on the website with photographs unless specific written permission is granted.
- Pupils full names will not be used anywhere on the website.
- Children who cannot be photographed will not be put on the website.

10. How will the ICT System security be maintained?

The school ICT systems will be reviewed regularly with regard to security. Virus protection will be installed and updated regularly. Security strategies will be discussed with the Local Authority particularly where a wide area network connection is planned.

LAN security issues include:

- The user must act reasonably. Loading non approved software could cause major problems. Passwords should be changed every six months.
- Cabling should be secure and wireless LAN's safe from interception.
- Servers must be located securely and physical access restricted.
- Virus protection for the whole network must be installed and current.