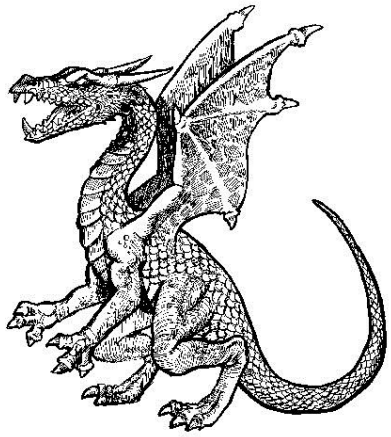
Southbury Primary School



Online Safety Policy
February 2019

Southbury Primary School
Online Safety Overview

A school's Online Safety Policy must cover the safe use of internet and electronic communications technologies such as mobile phones and wireless connectivity. The policy will highlight the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It will also provide safeguards and rules to guide staff, pupils and visitors in their online experiences.

Online Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.
The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security.

New technologies open up many exciting benefits and opportunities for learning and development but can also present risks. Wider access to technology via iPads/tablets, mobile phones, games consoles and other devices bring new challenges about controlling access and content.

Our Online Safety Policy has been written by the school. It has been agreed by the senior management team and approved by governors in 2019.
The Online Safety Policy will be reviewed annually by the Computing Coordinator or other senior member of staff.

Contents

Writing and reviewing the Online Safety policy .....
Teaching and learning .....
- Why the Internet and digital communications are important .....
- Internet use will enhance learning .....
- Pupils will be taught how to evaluate Internet content .....

Managing Internet Access .....
- Information system security .....
- E-mail .....
- Published content and the school web site .....
- Publishing pupil's images and work .....
- Social networking and personal publishing .....
- Managing filtering .....
- Managing videoconferencing & webcam use .....
- Managing emerging technologies .....
- Protecting personal data .....

Policy Decisions .....
- Authorising Internet access .....
- Assessing risks .....
- Handling Online Safety complaints .....

Communications Policy .....
- Introducing the Online Safety policy to pupils .....
- Staff and the Online Safety policy .....
- Enlisting parents' and carers' support .....

Appendix 1: Useful resources for teachers .....
Appendix 2: Useful resources for parents .....
Online Safety Audit – Primary .....

Writing and reviewing the Online Safety Policy

Rapid developments in electronic communications are having a profound effect on schools and the wider community. Our belief is that every pupil in the school can achieve in education through Computing and Internet use. The school has a duty to provide students with quality Internet access as part of their learning experience. In response to such advancements in the Computing curriculum and technology, pupil's use of the Internet must be safeguarded to ensure effective use of electronic communications.

Teaching and learning

Why the Internet and digital communications are important

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.

Access to a range of technology throughout the primary curriculum will enable pupils to prepare for a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology. Pupils use technology to find, explore, analyse, exchange and present information responsibly, creatively and without discrimination. Pupils learn how to employ technology to enable rapid access to ideas and experiences from a wide range of people, communities and cultures.

Internet use will enhance learning

The school Internet access has been designed expressly for pupil use and includes filtering as provided by The London Grid for Learning.

Pupils are supervised when using the internet.

Pupils and parents are informed what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils and staff must all sign an acceptable use agreement.

Children must agree to an acceptable use agreement each time they login to a school computer.

Pupils in Key Stage 2 will be given guidance in the effective use of the Internet in research.

Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
Pupils in Year 6 will be taught the importance of cross-checking information before accepting its accuracy and will learn about copyright and acknowledge the sources of information that they find online.
Pupils are asked to report unpleasant Internet content to the supervising adult. We have installed 'Hector Safety Button' as a safety feature on all school computers to assist with this.

Managing Internet Access

Information system security

School COMPUTING systems security will be reviewed
regularly. Virus protection will be kept updated.
Security strategies will be used according to the Local Authority guidance.

E-mail

Pupils may only use approved e-mail accounts where necessary on the school system.

In e-mail communication, pupils must not send emails to accounts not approved by the supervising adult.

Pupils must immediately tell a teacher if they receive offensive e-mail.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

The forwarding of chain letters is not permitted.

Published content and the school web site

Staff or pupil personal contact information will not generally be published. The contact details given online will be the school office and address.
The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully and the school will choose group photographs rather than full-face photos of individual children.
Pupils' full names will not be used anywhere on a school Web site or other online space, particularly in association with photographs.
Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site.
Work can only be published with the permission of the pupil and parents/carers.

Social networking and personal publishing

The school does not allow access to social networking sites by pupils at school unless a specific educational value is found, and will then educate pupils 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 when using such sites at home.
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 nicknames when using social networking sites.
Pupils will be advised not to upload videos onto YouTube or other media sharing sites.

Pupils are taught and reminded of Online Safety rules and expectations at the beginning of every Computing unit as well as being taught them explicitly in the Autumn term through Digital Literacy.

The school has an educational Twitter page. The page was designed to share ideas, show how we learn in the classroom and to keep Parent/Carers and friends of Southbury up to date with all that we do in school. The aim for this page is to stay connected with families and to explore learning on a new level through technology and social media. Parents/Carers have the opportunity to grant/deny permission for their child to be included on the Twitter page. A letter containing this permission and details about the Twitter page given to parent's March 2019.

Managing filtering

The school will work with the London Borough of Enfield Education, Children Services & Leisure Service and Enfield Safeguarding Board to ensure systems to protect pupils are reviewed and improved.
If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Leader/Technician/DSL.
Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing & webcam use

Videoconferencing will use the school broadband network to ensure quality of service and security.
Videoconferencing and webcams use will only be used by pupils for educational purposed and will be appropriately supervised by a responsible adult.

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.
Mobile phones are not allowed in school by pupils and will not be used during lessons or formal school time by staff (see mobile phone policy).
Staff will use a school phone where contact with pupils is required and use a school camera to capture photographs of pupils for website or school social media use.
Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories/
The appropriate use of any further Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Southbury Primary School aims to ensure that pupils and staff

information is treated lawfully and correctly. The school, and any person who handles personal data on behalf of the school, fully adheres to the General Data Protection Regulation.

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
• Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified unless written permission has been given.
• Pupils' full names or any other personal information will not be used anywhere on the website, particularly in association with photographs.
• Written permission from parents or carers will be obtained before images of pupils are electronically
published on any school website or social media.

Policy Decisions

Authorising Internet access

All staff must read and sign the "Staff Code of Conduct for COMPUTING" before using any school COMPUTING resource.
The school will maintain a current record of all staff and pupils who are granted access to the school COMPUTING systems.
At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
Parents will be asked to sign and return a consent form.
Any person not directly employed by the school will be asked to sign an "acceptable use of school COMPUTING resources" before being allowed to access the internet from the school site. In addition, any person logging onto a computer at school will have to agree to an acceptable use agreement.

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. Neither the school nor Enfield County Council can accept liability for any material accessed, or any consequences of Internet access.

The school should audit COMPUTING use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

Handling Online 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 of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure (see schools complaints policy)

Pupils and parents will be informed of consequences for pupils misusing the Internet.

Communications Policy

Introducing the Online Safety policy to pupils

Online 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.

A programme of training in Online Safety is in place, based on the materials available through MeOnline (KS1) and Cyberpass (KS2) on LGFL.

Online Safety training will be embedded within the Computing scheme of work at all stages. It is also taught explicitly over a half term.

Staff and the Online Safety policy

All staff will be given the School Online Safety Policy and its importance explained.

Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff that manage filtering systems or monitor COMPUTING use will be supervised by senior management and work to clear procedures for reporting issues.

Staff will always use a child friendly safe search engine when accessing the web with pupils.

Staff must always check with SLT before bringing in personal computer equipment including hard drives and the data stored must be checked/encrypted by the school's COMPUTING Technician.

Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school Web site.

The school will maintain a list of Online Safety resources for parents/carers including workshops run by 02 & NSPCC and have an annual meeting regarding Online safety.

The school will ask all new parents to sign the parent /pupil agreement and social media permission letter when they register their child with the school.

Parents will be informed by the school of any misuse or online activity that the school have been made aware of that may put a child in danger of exploitation.

Useful resources for teachers

LGFL –
Just 2 Easy (j2e)
Art skills for teachers
Web Teach Tutor
j2code
App maker
Our Online World
MeOnline
Cyberpass
Maths Raps
Talking Stories
Grammar Explained
Fairytales
Reading Zone Live
Maths toolbox

Espresso

Oscar's Adventures in the Online World eBook

Scratch/Scratch Jnr

Kahoot

Useful resources for parents

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Childnet
www.childnet-int.org/

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen
www.digizen.org/

National Online Safety
https://nationalonlinesafety.com/resources/

Net-aware
https://www.net-aware.org.uk/

NSPCC
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/talking-your-child-staying-safe-online/

NSPCC 02
https://guru.secure.force.com/O2DeskStoreLocator

Safer Internet Centre
https://www.saferinternet.org.uk/

Think U Know
www.thinkuknow.co.uk/

Online Safety Audit – Primary

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for Online Safety policy. Many staff could contribute to the audit including: Designated Child Protection Coordinator, SENCO, Online Safety Coordinator, Network Manager and Headteacher.

Has the school an Online Safety Policy that complies with Enfield guidance?	**Y/N**
Date of latest update (at least annual):	
The school Online Safety policy was agreed by governors on:	
The policy is available for staff at:	
The policy is available for parents/carers at:	
The responsible member of the Senior Leadership Team is:	
The responsible member of the Governing Body is:	
The Designated Child Protection Coordinator is:	
The Online Safety Coordinator is:	
Has Online Safety training been provided for both pupils and staff?	**Y/N**
Is there a clear procedure for a response to an incident of concern?	**Y/N**
Have Online Safety materials from CEOP and Becta been obtained?	**Y/N**
Do all staff sign a Code of Conduct for COMPUTING on appointment?	**Y/N**
Are all pupils aware of the School's Online Safety Rules?	**Y/N**
Are Online Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	**Y/N**
Do parents/carers sign and return an agreement that their child will comply with the School Online Safety Rules?	**Y/N**
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**Y/N**
Has a COMPUTING security audit been initiated by SLT, possibly using external expertise?	**Y/N**

Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y/N**
Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements (e.g. KCN, Regional Broadband Consortium, NEN Network)?	**Y/N**
Has the school-level filtering been designed to reflect educational objectives and approved by SLT?	**Y/N**