



# Springhead Primary School E-safety Policy

**January 2017**

## **Aims**

**1.1** We at Springhead Primary School recognise the Internet and other digital technologies provide a vast opportunity for children. More than any other mode of technology, the Internet and digital technologies allow all those involved in the education of children to promote creativity, stimulate awareness and enhance learning.

**1.2** Along with the desire for children to access every opportunity for learning, there will be the need to keep them safe from the dangers of the Internet, digital and mobile technologies. With this in mind, Springhead Primary School has created a policy that is aimed at developing not only a whole school approach to e-safety, but also an approach that seeks to protect children who access the Internet and digital technologies outside the school environment.

## **2.1 Writing and reviewing e-Safety Policy**

**2.1.1** The e-Safety policy is part of the safeguarding procedures in the school and relates to other policies including those for ICT, bullying and child protection. The school will appoint an e-Safety Coordinator who will be responsible for coordinating all e-Safety activities and issues.

**2.1.2** The e-Safety policy has been written by Springhead Primary School, building on Staffordshire guidance and Government guidance. This policy has been agreed by senior management and approved by governors.

The policy is reviewed annually by the e-Safety coordinator and the senior management team.

## **2.2 Teaching and Learning**

**2.2.1** The internet is an essential element in 21<sup>st</sup> 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. Using the Internet is part of the statutory curriculum and a necessary tool for staff and pupils.

**2.2.2** E-safety is covered as part of Computing / PHSE / other lessons and is regularly revisited. Key e-safety messages are reinforced throughout the year e.g. E-safety month/day. Pupils are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

**2.2.3** Internet access at Springhead Primary School is designed expressly for pupil use. We use RM SafetyNet+ filtering provided by Staffordshire Learning Network and Policy Central Enterprise (PCE), both are appropriate to the age of the children. As part of the Computing curriculum the children will be taught what Internet use is acceptable and what is not and given clear objectives for internet use. These objectives are displayed clearly on each computer when the children log on. The monitoring of this software is carried out by the E-safety co-ordinator.

**2.2.4** We at Springhead Primary School will ensure that the use of Internet derived materials by both staff and pupils complies with copyright law. Pupils will be taught the importance of cross-checking information before accepting its accuracy.

## **2.3 Managing Internet Access**

**2.3.1** The ICT systems security will be reviewed regularly by the e-Safety coordinator, the ICT technician and the senior management team. The ICT technician will ensure virus protection is updated regularly

**2.3.2** Children may only use approved e-mail accounts on the school system; they must immediately tell a member of staff if they receive an offensive e-mail. In e-mail communication, children must not reveal their personal details or those of others. The Telecommunications Act 1984, section 43 makes it an offence to send by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. All 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. The Acceptable Use Policy will be displayed near to all computers.

**2.3.3** On the School website only the school office contact details will be given online. Staff or pupil contact information will not be published. The headteacher will take overall editorial responsibility for the school website and ensure that content is accurate and appropriate.

**2.3.4** When publishing images of children we will take care to ensure that individual children cannot be identified or their images misused. Children's full names will not be used anywhere on the school Web site, 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.

**2.3.5** The staff at Springhead Primary School will educate children in the safe use of social networking sites; however these sites will not be accessible on school grounds. Children will be advised never to give out personal information of any kind which can identify them, their friends or their location. We will advise children and parents that using social networking sites brings a range of dangers.

**2.3.6 Springhead Primary** School will work with outside agencies such as CEOP to ensure the systems in place to protect pupils are reviewed and improved. If staff or children come across unsuitable on-line materials, the site should be reported to the e-Safety coordinator. The e-Safety coordinator and senior management team will ensure that regular checks of PCE e-monitoring software are made to ensure that the filtering systems are appropriate and effective.

**2.3.7** If using videoconferencing the educational broadband network should be used to ensure quality of service and security. Children should ask permission from the teacher before making or accepting a videoconference call. Videoconferencing and webcam use will be appropriately supervised for the children's age.

**2.3.8** Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The senior management team should be aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable materials and communications. Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

**2.3.9** Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

## **2.4 Policy Decisions**

**2.4.1** All staff must read and sign the 'Staff Acceptable Use' before using any school ICT resource. The school office will maintain a current record of all staff and children who are granted access to the school ICT systems. Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site. In KS1, access to the Internet will be by adult demonstration with directly supervised access to specific online materials.

**2.4.2 Springhead Primary** 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. The e-Safety coordinator will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate and effective.

## **2.5 Communications Policy**

**2.5.1** The e-Safety coordinator will ensure e-Safety rules will be displayed in all rooms where computers are used and they will be discussed with children regularly. Children will be informed that Internet use will be monitored using PCE e-monitoring software and appropriately followed up. A programme of training in e-Safety will be carried out and developed and led by the e-Safety coordinator. E-Safety training will be embedded within the ICT scheme of work.

**2.5.2** All staff will be given the School e-Safety Policy and its importance explained. Staff will be informed that Internet traffic can be monitored and traced to individual users. Staff will always use a child friendly search engine when accessing the Internet with children.

**2.5.3** 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 also maintain a list of e-Safety resources for parents/carers and hold Parent workshops to explain School Policy and discuss any concerns.

## **2.6 Internet Misuse**

**2.6.1** Should there be a complaint of Internet Misuse involving illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

These will be dealt with by the e-Safety coordinator and Child protection Officer using the flow chart from the Staffordshire Safeguarding Children's board which will be consulted and actions followed in line with the flow chart

**2.6.2** Any complaint about staff misuse of the Internet must be referred to the headteacher. Any complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

**2.6.3** Policy Central Enterprise detects potentially inappropriate content and conduct as soon as it appears on the screen, is typed in by the user or received by the user. A screen capture is taken of every incident detailing the time and date of capture, machine name, username and reason for capture. A weekly headline summary is produced from the system detailing captures of particular interest to alert the person monitoring the system. These particular violation will be investigated and dealt with in accordance to the Acceptable Use Policy (AUP), behaviour policy and other relevant school policies.

**2.6.4** Serious breaches of the PCE e-monitoring solution within school will be dealt with accordingly and investigation / action / sanctions will be the responsibility of the Headteacher.



## **SPRINGHEAD PRIMARY SCHOOL**

### **Email and Internet Use Good Practice**

#### **Rules for ICT Use**

We use the school computers and internet connection for learning.

These rules will help us to be fair to others and keep everyone safe.

- I will ask permission before entering any website, unless my teacher has already approved that site
- On a network, I will use only my own login and password, which I will keep secret
- I will not look at, change or delete other people's files
- I will not bring portable storage devices to use in school without permission
- I will only use the computers for school work and homework
- I will only email people I know, and at school only email people my teacher has approved
- The messages I send will be polite and sensible
- When sending email, I will not give my home address or phone number, or arrange to meet someone
- I will ask permission before opening an email or an email attachment sent by someone I do not know
- I will not use internet chat
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately
- I know that the school may check my computer files and may monitor the internet sites I visit
- I understand that if I deliberately break these rules, I could be stopped from using the internet or computers

# SPRINGHEAD PRIMARY SCHOOL

## Consent Form

### For Responsible Email and Internet Use

Child's Name: \_\_\_\_\_ (capitals please)      Class: \_\_\_\_\_

\*\*\*\*\*

#### Child's Agreement:

I have read and understand the school 'Email and Internet Use Good Practice – Rules for ICT Users'. I will use the computer system and internet in a responsible way and obey these rules at all times.

Child' Signature: \_\_\_\_\_      Date: \_\_\_\_\_

\*\*\*\*\*

#### Parent/Carer's Consent for Internet Access:

I have read and understood the school 'Email and Internet Use Good Practice – Rules for ICT Users' and give permission for my child to access the internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.

Parent/Carer Signature: \_\_\_\_\_      Date: \_\_\_\_\_

\*\*\*\*\*

#### Parent/Carer's Consent for Web Publication of Work and Photographs:

I agree that, if selected my child's work may be published on the school website.

I also agree that photographs that include my child may be published subject to the school rules that photographs will not clearly identify individuals.

Parent/Carer Signature: \_\_\_\_\_      Date: \_\_\_\_\_

Please Print Parent/Carer Name: \_\_\_\_\_