# STRATFORD PRIMARY SCHOOL

# E-Safety Policy

| | |
|---|---|
| **Date adopted by Governors:** | **January 2018** |
| **Date for policy review:** | **January 2020** |
| **Person responsible for review:** | **Mrs S McCormack** |
| **Signed by Chair of Governors** | **January 2018** |

## 1.0 Introduction

**1.1** Stratford Primary School recognises that the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

**1.2** The requirement to raise awareness in children and young people of the risks associated with inappropriate contact and behaviour via the internet and access to inappropriate content on the internet is addressed as part of the wider duty of care for all teachers. It is essential that all pupils are taught the relevant skills and strategies to remain safe when using the internet and related technologies and that they use these technologies appropriately. This may be as discrete internet safety lessons, as part of the ICT curriculum, or embedded within all curriculum work wherever it is relevant. Recognising the issues and planning accordingly will help to ensure appropriate, effective and safe pupil use.

**1.3** E-Safety depends on effective practice at a number of levels: Responsible ICT use by schools including all staff and students, as well as parents, governors and advisers;
encouraged by education and made explicit through published policies. Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use. Safe and secure broadband from the Warwickshire Broadband including the effective management of Websense filtering and Policy Central monitoring.

**1.4** As part of our commitment to learning and achievement, we want to ensure that the
Internet and other digital technologies are used to:

a) Raise educational standards and promote pupil achievement.
b) Develop the curriculum and make learning exciting and purposeful.
c) Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.
d) Enhance and enrich their lives and understanding.

**1.5** E-Safety encompasses Internet technologies and electronic communications such as mobile phones and tablet computers, as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

## 2.0 Safety

**2.1** E-Safety depends on effective practice at a number of levels:

• Responsible ICT use by all staff and students; encouraged by education and made explicit though published policies
• Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
• Safe and secure broadband from the inclusion of effective management of 'Web-Sense' filtering and 'Policy Central' monitoring through Warwickshire ICT Development Services.
• National Educational Network Standards and Specifications, (BECTA)

## 3.0 Teaching and learning

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

**3.2** How internet use will enhance learning
• The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
• Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use.
• Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
• Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

**3.3** Pupils will be taught how to evaluate Internet content
• If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to Warwickshire ICT Development Service, and where appropriate the school e-safety manager (ICT Manager).
• Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

## 4.0 Managing Internet Access

**4.1** Information system security
• The security of the school information systems will be reviewed regularly
• The school uses the Warwickshire Broadband with its firewall and filters.
• The school provides an addition level of protection through its deployment of Policy Central in partnership with Warwickshire ICT Development Services.

**4.2** E-mail
• Pupils may only use approved whole class e-mail accounts on the school system.
• Pupils must immediately tell a teacher if they receive offensive e-mail.

• Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
• Use of words included in the Policy Central 'banned' list will be detected and logged.
• In our school we will only use whole class e-mail accounts and the use of personal email accounts will be not allowed.
• E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
• The forwarding of chain letters is not permitted.

**4.3** Published content and the school web site
• The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
• The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

**4.4** Publishing staff and pupil's images and work
• Photographs that include pupils will be selected carefully
• Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
• Written permission from parents or carers will be obtained yearly where parents will be given the opportunity to consent to photographs of pupils being published on the school Web site.
• Pupil's work can only be published with the permission of the pupil and parents.
• Images of staff should not be published without consent.

**4.5** Social networking and personal publishing
• Social networking sites and newsgroups will be blocked unless a specific use is approved.
• Pupils are taught never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM (instant messenger) address, e-mail address, names of friends, specific interests and clubs etc.
• Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.

**4.6** Managing filtering
• The school will work in partnership with the Warwickshire ICT Development Service with advice from Becta to ensure filtering systems are as effective as possible.
• If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator. The 'Response to an incident of concern' procedure will be followed – see appendix 1.
• The ICT subject manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

**4.7** Managing videoconferencing
• IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet. Equipment connected to the

educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
• External IP addresses should not be made available to other sites.
• Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
• Videoconferencing should be supervised appropriately for the pupils' age.

**4.8** 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.
• Mobile phones are not be allowed in school during the working day.

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

## 5.0 Policy Decisions

**5.1** Authorising Internet access
• The school will maintain a current record of all staff and pupils who are granted Internet access.
• All users must read and abide by the acceptable ICT use policy before using any school ICT resource.
• 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; this will be part of the induction pack for new reception children / new starters.

**5.2** Assessing risks
• In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor WCC can accept liability for the material accessed, or any consequences of Internet access.
• The ICT subject manager will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

**5.3** 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 who should use the agreed WCC procedures.
• 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.
• Sanctions within the school discipline policy include:

– informing parents or carers;
– detentions or removal of Internet or computer access for a period.

**5.4** Community use of the Internet
• The school will liaise with users of the internet in school to establish a common approach to e-safety.
• Visitors to the school must use a guest log on code, given via ICT subject manager.
• The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice. This will link PSHE and ICT.

## 6.0 Communications Policy

**6.1** Introducing the E-safety policy to pupils
• Rules for Internet access will be posted in all networked rooms.
• Pupils will be informed that Internet use is monitored.
• An e-Safety awareness programme has been introduced to raise the awareness and importance of safe and responsible internet use.

**6.2** Staff and the E-Safety policy
• All staff have access to the School e-Safety Policy and its importance explained.
• Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

## 7.0 The Role of the Governing Body

**7.1** The governing body have a statutory responsibility for internet safety and security.

**7.2** Governors should develop an awareness of the issues and risks of using ICT in schools alongside the benefits.

**7.3** ICT / Internet safety should be reviewed regularly as part of the review of the school's health and safety and child protection policies

## 8.0 Enlisting parents' support

**8.1** Parents' attention will be drawn to the School e-Safety Policy in the weekly newsletters and the school website and portal.

**8.2** All new pupil intakes will be asked to sign an internet pupil agreement form (both parents and Children).

## 9.0 Development of this policy

**9.1** The ICT manager drafted this policy according to WCC guidelines given at the e-safety training course.

**9.2** Staff were given the opportunity to comment on the policy and make amendments.

**9.3** Discussions took part at a leadership team level.

**9.4** It is a statement of our whole school policy to e-safety and child protection.

## 10.0 Notes on the legal framework

**10.1** Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal.

**10.2** The law is developing rapidly and recent changes include:
• The 2003 Sexual offences Act has introduced new offences of Grooming and raised the age for making/distributing indecent images of children to 18.
• Offences regarding racial hatred are covered by the Public Order Act 1986

### 10.3 Possible Offences

**A. Sexual Offences Act 2003**
• **Grooming** – If you are over 18 and have communicated with a child under 16 at least twice (including by phone or Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

• **Making indecent images** – it is an offence to take, make, distribute, show, advertise indecent images of a child under 18. (NB to view an indecent image on your computer means that you have made a digital image.)

• **Causing a child under 16 to watch a Sexual Act** – to intentionally cause a child to watch someone else taking part in sexual activity, including looking at images such as videos, photos or webcams, for your own gratification

**B. Relevant Legislation**

• **The Computer Misuse Act 1990** - makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

• **Public Order Act 1986** – offence to possess, publish, disseminate material intended to/likely to incite racial hatred.

• **Communications Act 2003** –

There are 2 separate offences under this act:

a) sending by means of a public electronic communications network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.
b) sending of a false message or persistently making use of a public electronic communications network for the purpose of causing annoyance, inconvenience or needless anxiety.

• This wording is important because the offence under a. is complete when the message has been sent - no need to prove any intent or purpose. It is an offence under b. to keep using the network for sending any kind of message irrespective of content if for the purpose of causing annoyance etc.

• **Malicious Communications Act 1988** – offence to send a letter, electronic communication or article which is indecent or grossly offensive, threatening or false information with intent to cause distress or anxiety to the recipient.

• **Copyright, Design and Patents Act 1988** - it is an offence to use unlicensed software

• **Protection of Children Act 1978** - The law on images of child abuse is clear. It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom.

• **Obscene Publications Act 1959 and 1964** - defines “obscene” and related offences.

• **Protection from Harassment Act 1997**
• Section 2 - A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
• Section 4 - A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

B. **Sex Offences Act 2003 Memorandum of Understanding**
Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003.

The aim of this memorandum is to help clarify the position of those professionally involved in the management, operation or use of electronic communications networks and services who may face jeopardy for criminal offences so that they will be re-assured of protection where they are acting to combat the creation and distribution of images of child abuse.

This memorandum has been created within the context of child protection, which will always take primacy.
The MOU: http://www.iwf.org.uk/police/page.22.213.htm