Outwoods Primary School

Written: July 2010
Re-Ratified: July 2016
Review Date: July 2017

e-safety policy

2.1 Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- The School has an e-Safety Coordinator.
- Our e-safety Policy has been written by the School, building on the Kent e-safety policy and government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy was revised by: Helen Hutchinson
- It was approved by the Governors on: July 2016
- The next review date is (at least annually): July 2017

2.2 Teaching and Learning

2.21 Why the Internet and digital communications are important

- The Internet is an essential element in the 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2.3 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.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information to a wider audience.

2.2.4 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 laws.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

2.3 Managing Internet Access

2.3.1 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.

2.3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- The forwarding of chain letter is not permitted by pupils.

2.3.3 Published content and the school website

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

2.3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using 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 on-line 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.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

2.3.5 Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

2.3.6 Managing filtering

- The school will work with the Staffordshire County Council 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 e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- PCE has been paced on the network and all staff laptops and will be checked by senior leadership.

2.3.7 Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

2.3.8 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.
- 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 will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones will be kept under review.

- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

2.3.9 Protecting personal data

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

2.4 Policy Decisions

2.4.1 Authorising Internet Access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT 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.

2.4.2 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 SCC can accept liability for any material accessed, or any consequences of Internet access.
- The school should 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.

2.4.3 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.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. (The SCC e-Safety Policy has a flowchart of responses to an incident of concern.)
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)

2.4.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

2.5 Communications Policy

2.5.1 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.
- A programme of training in e-Safety will be developed.
- Children will be taught about e-safety within all teaching and have e-safety focused sessions each term using a whole school approach.
- Children will participate in a whole school e-safety day to coincide with the national Safer Internet Day.

2.5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff will be given regular e-safety training keeping them updated with resources and procedures.
- 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 ICT 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 will teach children about e-safety and the different aspects it includes. The resources and ideas will come from a scheme of work provided by the e-safety co-ordinator.

2.5.3 Enlisting parents' and carers' support

- 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 and as these are updated parents will be made aware.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.
- E-Safety training/updates will be provided for parents on a regular basis.

2.5.6 Use of mobile phones and cameras in school:

Staff, visitors, volunteers and students are NOT permitted to use their own mobile phones or cameras to take or record images of children.
Mobile phones should be turned off, must not be carried around in staff pockets and should be left with personal belongings in lockers, staffroom or the school office (during school hours).
Visitors may only use their phones in the foyer or outside the building.
Early Years staff are **NOT** permitted to have mobile phones in the Early Years Unit - they should be left in the school office or staffroom and can be collected at lunchtimes and/or the end of the school day.
The school mobile phones are available for use on educational visits.

Appendix 1: Internet use – Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks, webquest UK, Launchpad365
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids, Yahooligans, CBBC Search, Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	RM EasyMail SuperClubs Plus School Net Global Kids Safe Mail
Publishing pupils' work on school and other websites	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils' work should only be published on 'moderated sites' and by the school administrator.	Making the News SuperClubs Plus Headline History National Education Network Gallery
Publishing images including photographs of pupils	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil	Making the News SuperClubs Plus Learninggrids Museum sites, etc. Digital Storytelling

	by name. Staff must ensure that published images do not breach copyright laws.	BBC - Primary Art National Education Network Gallery
Communicating ideas within chat rooms or online forums	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Plus FlashMeeting
Audio and video conferencing to gather information and share pupils' work	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	FlashMeeting National Archives "On-Line" Global Leap JANET Videoconferencing Advisory Service (JVCS)

Appendix 2: Useful resources for teachers

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

Becta
http://schools.becta.org.uk/index.php?section=is

Chat Danger
www.chatdanger.com/

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/

Kent e-Safety Policy and Guidance, Posters etc
www.clusterweb.org.uk/kcn/e-safety home .cfm

Kidsmart
www.kidsmart.org.uk/

Kent Police – e-Safety
www.kent.police.uk/Advice/Internet%20Safety/e-safety%20for%20teacher.html

Think U Know
www.thinkuknow.co.uk/

Safer Children in the Digital World
www.dfes.gov.uk/byronreview/

Appendix 3: Useful resources for parents
Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD
http://publications.teachernet.gov.uk

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

Kent leaflet for parents: Children, ICT & e-Safety
www.kented.org.uk/ngfl/ict/safety.htm

Parents Centre
www.parentscentre.gov.uk

Internet Safety Zone
www.internetsafetyzone.com

Appendix 3: 360 Safe e-safety review tool

The school use the 360 safe e-safety review tool to review its e-safety policy and practices. Through this tool the school will continue to implement new e-safety practices where required.

Signed . . . . . Dated . . . . . .