E-Safety Policy

Stonebridge Primary School
December 2009

Contents

E-Safety Policy

"Children and young people need to be empowered to keep them-selves safe – this isn't just about a top-down approach. Children will be children – pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim." Dr Tanya Byron

E-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, Anti-Bulling, Curriculum, Data Protection and Security.

PHILOSOPHY

As a school we aim to:

- Protect pupils, so far as is reasonably practicable, from harm by teaching them how to use technology safely.
- Make clear to pupils, staff and parents the school's expectations regarding the use of ICT.
- Maximise the educational and social benefit that can be obtained by exploiting the opportunities offered by the use of ICT, whilst minimising any associated risks.
- Form part of the protection from legal challenge, relating to the use of ICT.

PRINCIPLES

Our school e-safety policy is built on the following three core principles:

Educating young people to be responsible users of ICT

- In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.
- Pupils need to know how to react if they come across inappropriate material and they should not give out personal information such as their address and telephone number to strangers or publish this on the internet.

- They should also be educated to critically evaluate the quality of the material they find on the internet.

Guided educational use

- Curriculum ICT use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful ICT use will also reduce the opportunities for activities of dubious worth.

Regulation and control

- Internet safety depends on all staff, governors, advisers, parents and the pupils themselves taking responsibility for the use of internet and other communication technologies such as mobile phones.

- Strategies to help to ensure responsible and safe use of internet is selected and effectively monitored.

- Staff, parents and the pupils themselves are encouraged to remain vigilant.

PROCEDURES

1. Regularly check with Becta for updated e-safety advice:

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

2. Pupils will have opportunity to discuss Rules for Responsible Internet Use

The importance of internet use

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Benefit of Internet use to Education

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of Networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DCSF; access to learning wherever and whenever convenient
  (See Appendix F- For Recommended Internet E- Safety Sites)

3. The curriculum context being planned for internet use to enhance learning.

Internet Use Enhancing Learning

- The school Internet access will be designed expressly for pupil use and includes 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.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.
-

4. Ensure that Vigilance and supervision is an essential strategy.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the e-safety coordinator or network manager.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use approved 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.
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organizations should be written carefully and authorized before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking

- The school blocks/filters access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals
- Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with the Local Authority, Becta and the Internet Service Provider to ensure filtering systems are as effective as possible.

Video Conferencing

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

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 will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

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 head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully
- Pupils' full names will not be used anywhere on the Web site or Blog, 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.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

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

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the local authority can accept liability for the 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.

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 head teacher.
- 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.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.
  (See Appendix A)

5. Communication of the Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

  (Appendix B)

Staff

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff Acceptable Use Policy signed by all members of staff.
  (Appendix D)

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, letter to parents (Appendix C) and on the school Web site.

Referral Process – Appendix A

E-Safety Rules– Appendix B1 & B2

Letter to parents – Appendix C

Staff Acceptable Use Policy – Appendix D

Staff Information Systems Code of Conduct – Appendix E

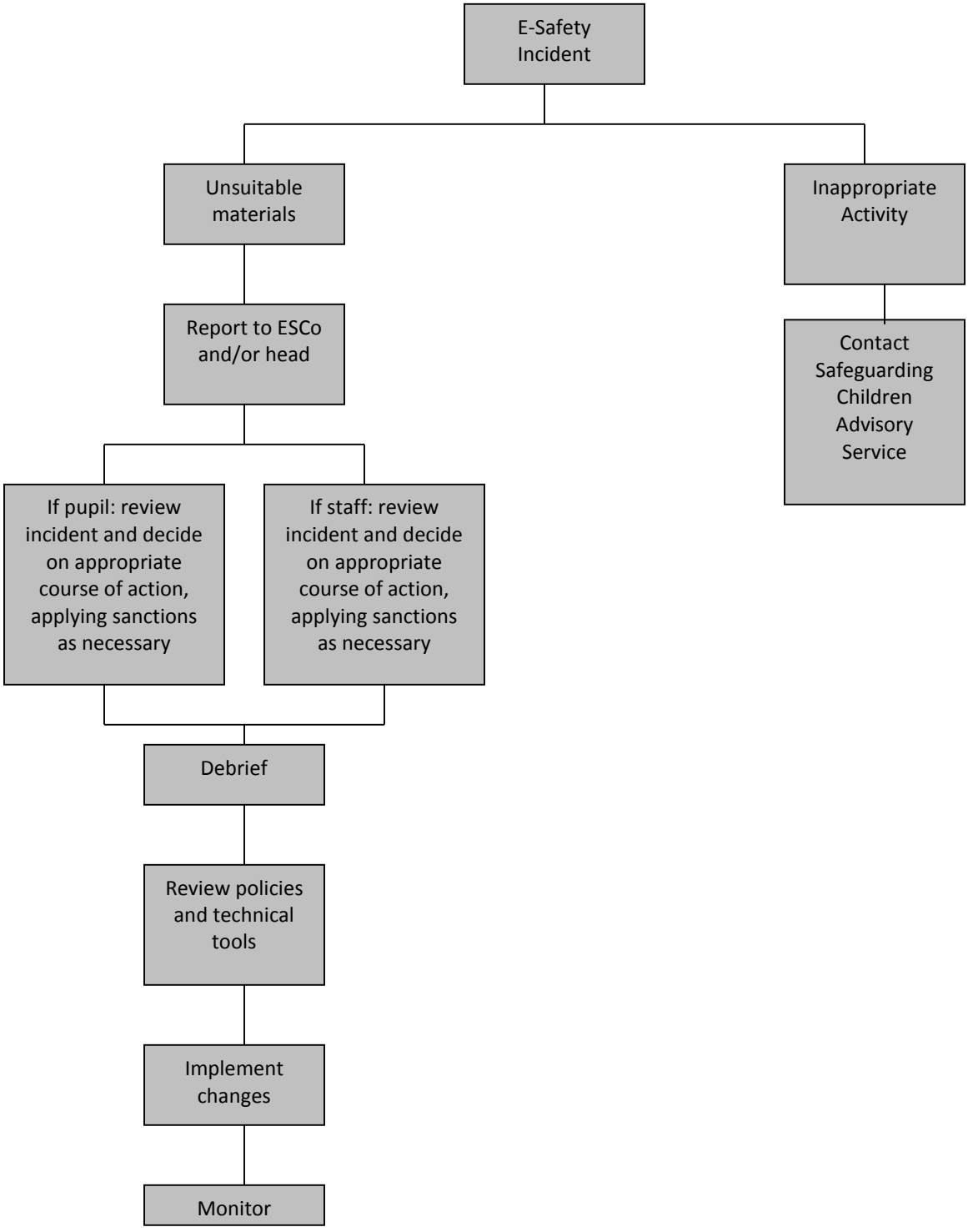
Rules For Responsible Internet Use-Appendix F

E-Safety Websites -Appendix G

E-Safety Self Audit – Appendix H

Appendix A

Flowchart for responding to e-safety incidents in school



E-Safety Rules

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorized account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorized use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorized or unlawful text, imagery or sound.

Adapted from Becta – E-safety

Key Stage 1

Think then Click

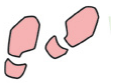
These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.



We can send and open emails together.

We can write polite and friendly emails to people that we know.

B. Stoneham & J. Barrett

Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

E-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the 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.

Signed:	**Date:**
Please print name:	

Please complete, sign and return to the school

THE STONEBRIDGE SCHOOL

ACCEPTABLE USE POLICY FOR STAFF AND VISITORS

Use of Internet and Electronic Mail

Policy Aim

The Stonebridge School makes every effort possible to provide you with access to the internet and electronic mail system in order to assist you with teaching and learning, staff development and communication needs. The policy is in place to protect the school, the schools employees, pupils and visitors (who have access to the classroom computers and the ICT suite). Please read the E- safety /AUP before signing the agreement below.

I have read and understood the E- safety/ AUP fully and agree to Stonebridge School's policy and terms of use

Internet

I agree that:

- I understand that if I accidentally breach this Policy whilst acting in good faith and in the course of my duties I MUST notify the ICT co-ordinator IMMEDIATELY so that action can be taken to prevent or minimise damage.
- I will not copy software files from the internet. No executable files should be copied from the internet.
- Downloads must only be carried out by a member of staff who is capable of ensuring that it is not faulty, is not infected with a virus and that all copyright requirements are met.
- I will not access any sites or download or print any files displaying material that I know to contravene the School's internet policy or Equal Opportunities Policy.
- I will not access any sites which provide a discussion or "chat" forum which does not fit the schools or London borough of Brent's uses.
- I will not access any sites which provide a discussion or "chat" forum which does not fit the authorised uses listed above,
- I will not order any goods via the Internet without consulting my line manager. *(please note that to do so may result in a breach of the formal procurement requirement in Financial Regulations),*
- I will not respond to surveys on the Internet on behalf of the School without consulting the ICT coordinator or head teacher.
- I will not open a subscription account on the Internet on behalf of the School without express permission of the head teacher.
- I will not allow anyone other than an employee of the school to use the Internet via the PC or laptop I am using.
- I will not use electronic mail for communication other than for purposes set out in the school's policy.
- I will not leave PCs or laptops in a state where it would be possible for someone other than the normal user (or other legitimate user) to access the Internet,
- I will not leave a PC unattended whilst it is on the Internet.
- I will not reveal my own (or any other person's) personal details e.g. Home address, telephone number, E-mail address etc over the Internet.

Electronic Mail

I agree that:

- Electronic mail should only be used in the course of my work as a school employee even if this account is used outside work hours or premises.
- Electronic mail is not a person-to-person communication and that I will always use appropriate language.
- Use of electronic mail to send or forward chain letters or any material which may contravene School policies (e.g. jokes, pictures of a racist or sexist nature) is not acceptable.
- Messages will only be copied (i.e. cc or bcc) to people where it is of direct relevance.
- That any unwanted electronic mail messages will be deleted from my INBOX, Sent and Trash folders.

PRINT NAME_____ **Signed** _____ **Date** _____

Staff Information Systems Code of Conduct

To ensure that staffs are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the head teacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorized use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorized or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Initials: …….. Date: ……

Accepted for school: …….. Initials: …… Date: ……

RULES FOR RESPONSIBLE INTERNET USE

The school has installed computers and Internet access to help our learning.
These rules will keep everyone safe and help us be fair to others.

1. I will only access the system with my own login and password, which I will keep secret
2. I will not access other people's files
3. I will only use the computers for school work and homework
4. I will not bring in floppy discs or other portable storage discs / keys, unless I have been given permission
5. I will ask permission from a member of staff before using the Internet
6. I will only email people I know, or my teacher has approved; the messages I send will be polite
7. I will not give anyone my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission
8. I will report any unpleasant material or messages sent to me and understand my report will be confidential and would help protect other pupils and myself
9. I understand that the school may check my computer files and may monitor the Internet sites I visit

I have read the above rules and responsibilities and agree to follow them

NAME: _____ **CLASS**_____

SIGNED: _____ **DATE**_____

E-Safety Websites

LGFL **ALL**
http://cms.lgfl.net/web/lgfl/safety

Think U Know (CEOP) **ALL**
http://www.thinkuknow.co.uk/

Cyber bullying **ALL**
http://www.digizen.org/cyberbullying/film.aspx

BBC Chat Guide **Y5**
http://www.bbc.co.uk/chatguide

Bullying Online **Y6**
http://www.bullying.co.uk

CBBC – Stay Safe **Y2**
http://www.bbc.co.uk/cbbc/help/safesurfing

CyberQuoll **Y4**
http://www.cyberquoll.com.au

Cyber smart Kids Online **Y5**
http://www.cybersmartkids.com.au

Netty's World **Y1 & 2**
http://www.nettysworld.com.au

FKBKO – For Kids by Kids Online **Y6**
http://www.fkbko.co.uk

Hector's World TM **Y1**
http://www.hectorsworld.com

iKeepSafe.org **Y4**
http://www.ikeepsafe.org

Internet Proficiency Scheme for Key Stage 2 pupils **Y6**
http://www.gridclub.com/teachers/t_internet_safety.html

Internet Safety Zone **Y5**
http://www.internetsafetyzone.com/kids

Kid smart **Y3**
http://www.kidsmart.org.uk/yp/under11

NetSmartzKids **Y1**
http://www.netsmartzkids.org

PHONE brain **Y6**
http://www.phonebrain.org.uk

QUICK: The Quality Information Checklist **Y6**
http://www.quick.org.uk

Safe Surfing with Doug **Y4**
http://www.disney.co.uk/DisneyOnline/Safesurfing

Smart Surfers **Y5**
http://www.smartsurfers.co.uk

Staying SMART Online **Y4**
http://www.kidsmart.org.uk/stayingsmart

Surf Swell Island: Adventures in internet safety **Y5**
http://disney.go.com/surfswell

Byron review **ALL**
http://www.dcsf.gov.uk/byronreview/

Foundation Stage info

http://foundation.e2bn.org/index.php?option=com_content&task=view&id=110&Itemid=32

E-Safety Audit

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place.

Has the school an e-Safety Policy that complies with CYPD guidance?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The designated Child Protection Teacher/Officer is:	
The e-Safety Coordinator is:	
Has e-safety training been provided for both pupils and staff?	Y/N
Is the Think U Know training being considered?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y/N
Have school e-Safety Rules been set for pupils?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access.	Y/N
Has the school filtering policy been approved by SMT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N