LEAVENING COMMUNITY PRIMARY SCHOOL

E-Safety Policy (2015)

Member of staff responsible: Jessica Skelton

Focus Group responsible:

Approved by Governors on:

Review Date: Autumn 2017

Chair of Governors: Neil Audsley

Headteacher: Sian Mitchell/ Martin Popplewell

Staff member: Jessica Skelton

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: November 2015	
The Policy was agreed by governors on:	
The Policy is available for staff on: Teachers server/Staff room	
And for parents: hard copy upon request /available on website	

The designated Child Protection Teacher/Officer is: Sian Mitchell/Martin Popplewell	
The e-Safety Coordinator is: Jessica Skelton	
Has e-safety training been provided for both pupils and staff?	**Y**/N **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 on computers? On desktops, in classrooms, Learning Zone, hall	**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 governors?	**Y**/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y**/N

Leavening Primary School

E-Safety Policy 2015

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.

This school has a duty to provide pupils with access to quality learning using internet technologies and electronic communications and, with this, the responsibility to ensure that this learning takes place safely.

This e -Safety policy highlights our commitment to e-safety and acknowledges its part in the school's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirements to keep pupils safe in the 'Every Child Matters' agenda and operates in conjunction with other policies such as Safeguarding and Child Protection, and ICT curriculum policy.

Good Habits

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

- Responsible ICT use by all staff and pupils; 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 including the effective management of content filtering.

Why is Internet Use Important?

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.

How does Internet Use Benefit 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 DFE;
- access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are 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, both within lessons and in after school clubs.
- 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.

Managing Internet Access

- All staff must read and sign the 'Staff Acceptable Use Agreement' before using any school ICT resource.
- Parents understand that pupils will be provided with supervised Internet access.
- E-Safety rule Posters will be displayed on the desktop of each pupil laptop, as reminders for pupils.
- 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.

- All children must understand that if they see an unacceptable image on a computer screen, they must lower the screen (laptop/ipad) or turn off the screen, and then report immediately to a member of staff.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- Children will be taught about the risk of Online Bullying, how to avoid it and what to do if it happens, during lessons on ICT Safety.
- The teaching of Internet safety is included in the school's ICT Scheme of Work, but all teachers within all year groups are including Internet safety issues as part of their discussions on the responsible use of the school's computer systems.

Social Networking

- Schools should block/filter 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 and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils and only moderated social networking sites should be used for this age range. Parents will be informed about that the minimum age for accessing most well-known sites is 13 (Y8).

Staff Guidance on the use of Social Networking and messaging systems

- The school recognises that many staff will actively use Facebook, Twitter and other such social networking, blogging and messaging services. It is recognised that some such services may have an appropriate application in school. However, where such activities are planned, a separate account should be set up for the purpose, and there should be no connection made between personal and school accounts used for educational purposes. Any such accounts and activities should be approved by the Head Teacher prior to use.

- Although these networks are used by staff in their own time, staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks. Staff are encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.
- **It is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors.**
- Staff are required to follow theses guidelines and demonstrate acceptable conduct at all times when using the school's IT systems and also act in a professional manner when accessing the internet from home. The school's and Local Authority Disciplinary Procedures will be used in the case of misuse or unprofessional conduct

Filtering

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

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 by staff for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages, files by Bluetooth or any other means is forbidden.
- Staff are encouraged to use a school phone where contact with pupils is required.
- 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.

Published Content and the School Web Site

- The school address, email and telephone number are the only contact details shared on the school website. Staff and pupils personal information will not be published.

- The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

The aim of the school's web site is to reflect the diversity of activities, individuals and education that can be found at Leavening Primary School. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the Internet, the following principles must be followed:

- Photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on the Web site / Learning Platform, in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- No link should be made between an individual and any home address (including simply street names).

For more information about the safe use of children's images at Leavening Primary School, see separate policy.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Advice from the Local Authority regarding new security strategies will be needed and relevant policies will be reviewed and updated.

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 York City

Council can accept liability for the material accessed, or any consequences of Internet access.

- The school will review ICT use annually to establish if the e-safety policy is adequate, effective or in need of modification and that the implementation of the e-safety policy is appropriate.

Community Use of the Internet

- The school will develop further guidance if the school's network and IT equipment has a community use.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by the Head teacher.
- 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.

Use of ICT Equipment

The computer system is owned by the school. "The computer system" means all computers and associated equipment in use by the school, whether part of the school's integrated network or stand-alone, or taken offsite. The school provides portable ICT equipment such as laptop computers, voice recorders, ipads and digital cameras to enhance the children's education. This also allows staff to make efficient use of such equipment in order to enhance their own professional activities.

- The installation of software or hardware unauthorised by the school, whether legitimately licensed or not, should be checked with either the ICT technician, Computing Leader or Headteacher before proceeding.
- The school reserves the right to examine or delete any files that may be held on its computer systems and to monitor any Internet sites visited.
- All personal data held on the school's network is subject to the Data Protection Act 1998 and the school's Data Protection Policy.
- Equipment such as Laptop computers are encouraged to be taken offsite for use by staff in accordance with this Acceptable Use Policy.
- Any costs generated by the user at home, such as phone bills, internet connection, printer cartridges etc. are the responsibility of the user.
- If an individual leaves the employment of the school, any equipment must be returned.
- Care should be taken over the use of USB pens, re-writeable CDs etc to transfer data from external computer systems. Where information has

been downloaded from the internet, or copied from another computer, wherever possible, it should be emailed to school to ensure that it undergoes anti-virus scanning.

- Staff may install software on laptops to connect to the Internet from home. Advice may need to be taken before attempting this.
- **Where data of a personal nature such as school reports, IEPs, correspondence, photographs and assessment data is taken home on a school laptop or other storage device, it must be recognised that this data comes under the Data Protection Act and is subject to the school's Data Protection Policy. Care must therefore be taken to ensure its integrity and security. If data is transferred to home computers it should be treated sensitively and removed from the hard drive and any portable device including USB pens and memory cards as soon as is possible.**

Communication of Policy

Pupils

- Rules for Internet access are on the desktops of all laptops.
- Pupils will be informed that Internet use will be monitored.

Staff

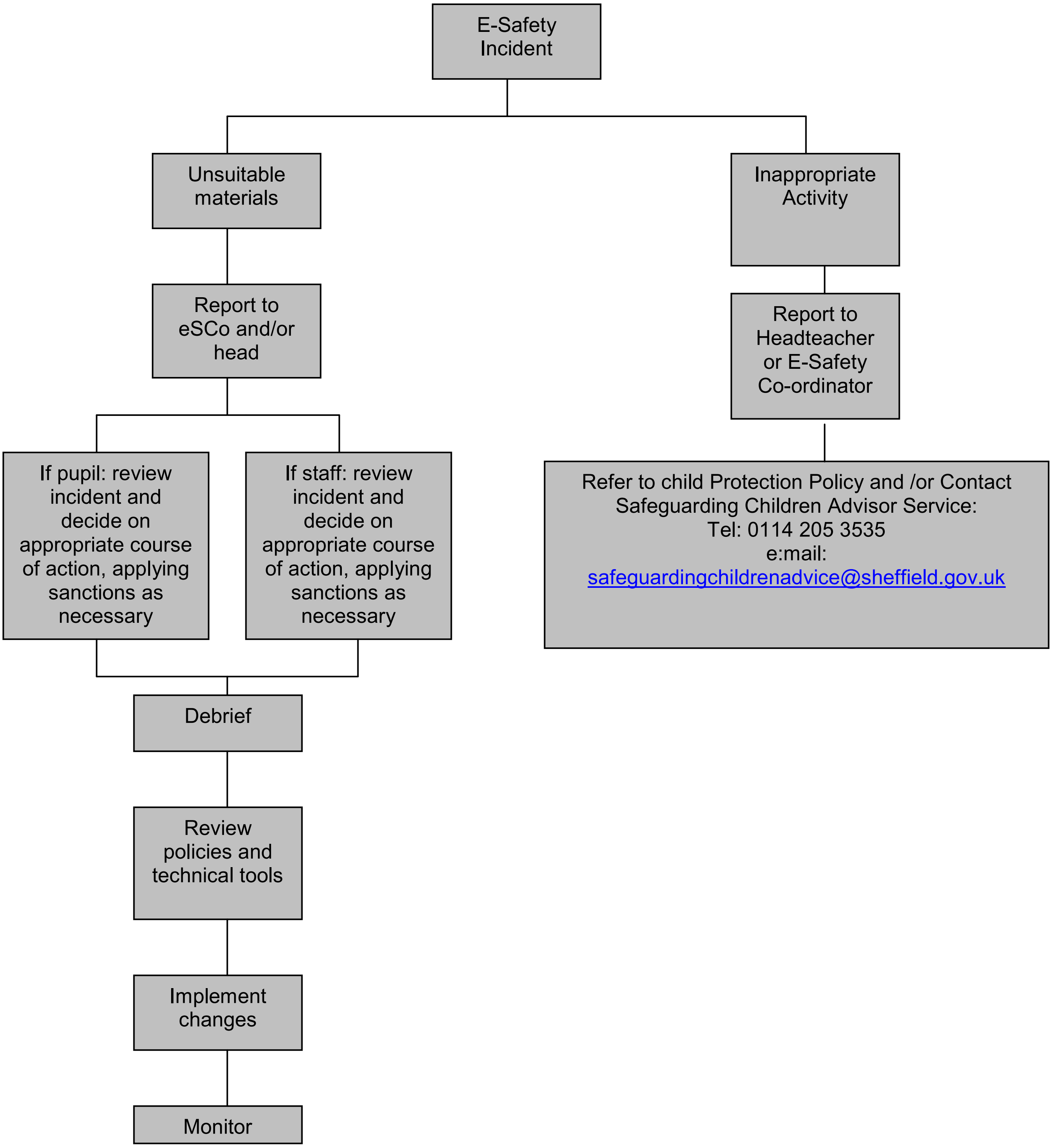
- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff to read and remain aware of the Staff Acceptable use Policy.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in School / Class newsletters, the school Web site and through ICT / E-Safety awareness evenings.
- The school will provide guidance and a list of E-Safety resources for parents/carers.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

Appendix A

Flowchart for responding to e-safety incidents in school


E-Safety Incident
Unsuitable materials
Inappropriate Activity
Report to eSCo and/or head
Report to Headteacher or E-Safety Co-ordinator
If pupil: review incident and decide on appropriate course of action, applying sanctions as necessary
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Refer to child Protection Policy and /or Contact Safeguarding Children Advisor Service:
Tel: 0114 205 3535
e:mail:
safeguardingchildrenadvice@sheffield.gov.uk
Debrief
Review policies and technical tools
Implement changes
Monitor

Adapted from Becta – E-safety 2005

Appendix B

Useful resources for school staff

BBC Newsround Staying Safe Online
http://www.bbc.co.uk/newsround/13910067
The Becta Review 2006
http://dera.ioe.ac.uk/1427/1/becta_2006_bectareview_report.pdf
Childnet
http://www.childnet.com/
Child Internet Safety Centre
http://www.ceop.police.uk/
Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/
Digizen
www.digizen.org/
Kidsmart
www.kidsmart.org.uk/
Think U Know
www.thinkuknow.co.uk/
UK Council for Child Internet Safety
http://www.gov.uk/government/groups/uk/government/groups/uk-council-for-child-internet-safety-ukccis

Useful resources for parents

Family Online Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk
Internet Safety Zone
www.internetsafetyzone.com
Childnet Know it All
http://www.childnet.com/resources/kia
Think U Know
http://www.thinkuknow.co.uk/parents/
Kidsmart
http://www.kidsmart.org.uk/parents

Acceptable Use Policy for All Staff - including temporary or supply staff and visitors to school.

As a member of staff, either temporary or permanent, or a visitor to the school I recognise that it is my responsibility to follow school e-Safety procedures and that I have a responsibility to ask for advice if I am not sure of a procedure.
I confirm that I will use all electronic communication equipment provided by the school, and any personal devices which I bring into in school, in a responsible manner and in accordance with the following guidelines:

- During lesson time, I will only use the school network for the purpose I have been given access, related to the work I am completing in the school. If accessing the internet outside of lesson times, I will be selective and responsible regarding my internet use.
- I will not use my personal mobile phone or other electronic equipment to photograph or video pupils.
- I will not publish photographs or videos of pupils without the knowledge and agreement of the school or the parents of the pupils concerned.
- I will not give my personal contact details such as email address, mobile phone number etc to any pupil in the school. Contact will always be through a school approved route.
- I will respect system security and I will not disclose any password or security information to anyone, other than an authorized system manager.
- I will take all reasonable steps to ensure the safety and security of school ICT equipment, including ensuring that any personal devices or memory devices I use are fully virus protected and that protection is kept up to date.
- I will only use my personal mobile phone during non-teaching time unless on a school trip or when the school phone is already in use. My phone will be kept on silent mode during lessons, except in an emergency situation.
- I will report any accidental access to material which might be considered unacceptable immediately to a senior member of staff and ensure it is recorded.
- I will report any incidents of concern regarding children’s safety (including unsuitable materials or inappropriate activity) to the E-Safety Coordinator, the Designated Child Protection Coordinator or Head teacher.

- If I have access to any confidential school information, pupil information or data it will only be removed from the school site temporarily (eg. when writing reports), and it will be stored on a portable device, not saved to the hard drive of any personal computers. When it is no longer needed, it will be removed from the portable device. I will report immediately any accidental loss of confidential information to a senior member of staff so that appropriate action can be taken.
- I will respect copyright and intellectual property rights.
- I understand that I have a duty of care to ensure that students in school use all forms of electronic equipment and devices safely and should report any inappropriate usage to a senior member of staff.
- I will not publish or share any information I have obtained whilst working in the school on any personal website, blog, social networking site or through any other means, unless I have permission from the school.
- I understand that the school may monitor or check my use of ICT equipment and electronic communications to ensure policy compliance.