Stocksbridge Nursery Infant School

eSafeguarding Policy

Policy adopted: May 2019

Policy review date: May 2020

eSafeguarding Policy Rationale

New technologies have become integral to the lives of children and young people in today's society. The internet and other digital information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside school. eSafeguarding 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 eSafegaurding policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security.

Good Habits

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

- Responsible ICT use by all staff, parents 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 from the Yorkshire and Humberside Grid for Learning including the effective management of content filtering.
- National Education Network standards and specifications.

Roles and responsibilities

We believe that eSafeguarding is the responsibility of the whole school community and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching

E-Safety Audit – Primary Schools

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**
Date of latest update: May 23rd 2019	
The Policy was agreed by governors on:	
The Policy is available for staff at: Non-Curricular Policy File, staff room	
And for parents at: Non-Curricular Policy File, parent shelves, reception	
The designated Child Protection Teacher/Officer is: Mrs Jane Townsend	
The e-Safety Coordinator is: Mrs Ruth Heavens	
Has e-safety training been provided for both pupils and staff?	**Y**
Is the Think U Know training being considered?	**N**
Do all staff sign an ICT Code of Conduct on appointment?	**Y**
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	**Y**
Have school e-Safety Rules been set for pupils?	**Y**
Are these Rules displayed in all rooms with computers?	**Y**
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access.	**Y**
Has the school filtering policy been approved by SMT?	**Y**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y**

Contents

Sheffield Children and Young Peoples' Directorate acknowledge the assistance of Kent County Council in providing content in this document.

School e-Safety Policy

The school will appoint an e-Safety coordinator. In many cases this will be the Designated Child Protection Officer as the roles overlap.

The e-safety co-ordinator at Stocksbridge Nursery Infant School is Mrs R Heavens

Our e-Safety Policy has been written by the school, building on the Sheffield Children and Young Peoples' Directorate and Government guidance. It has been agreed by the senior management team and approved by governors.

The e-Safety Policy will be reviewed annually. This policy will next be reviewed Summer 2020

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 DCSF; access to learning wherever and whenever convenient.

How can Internet Use Enhance 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.

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 organisations 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.

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 should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. 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

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- 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 on the school premises whilst children are still on the premises. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone when off site where contact with school is required.

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, ICT Co-ordinator or ICT technician will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- 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 2018.

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 Sheffield City Council 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 headteacher.
- 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.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- 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.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

Referral Process – Appendix A

E-Safety Rules– Appendix B

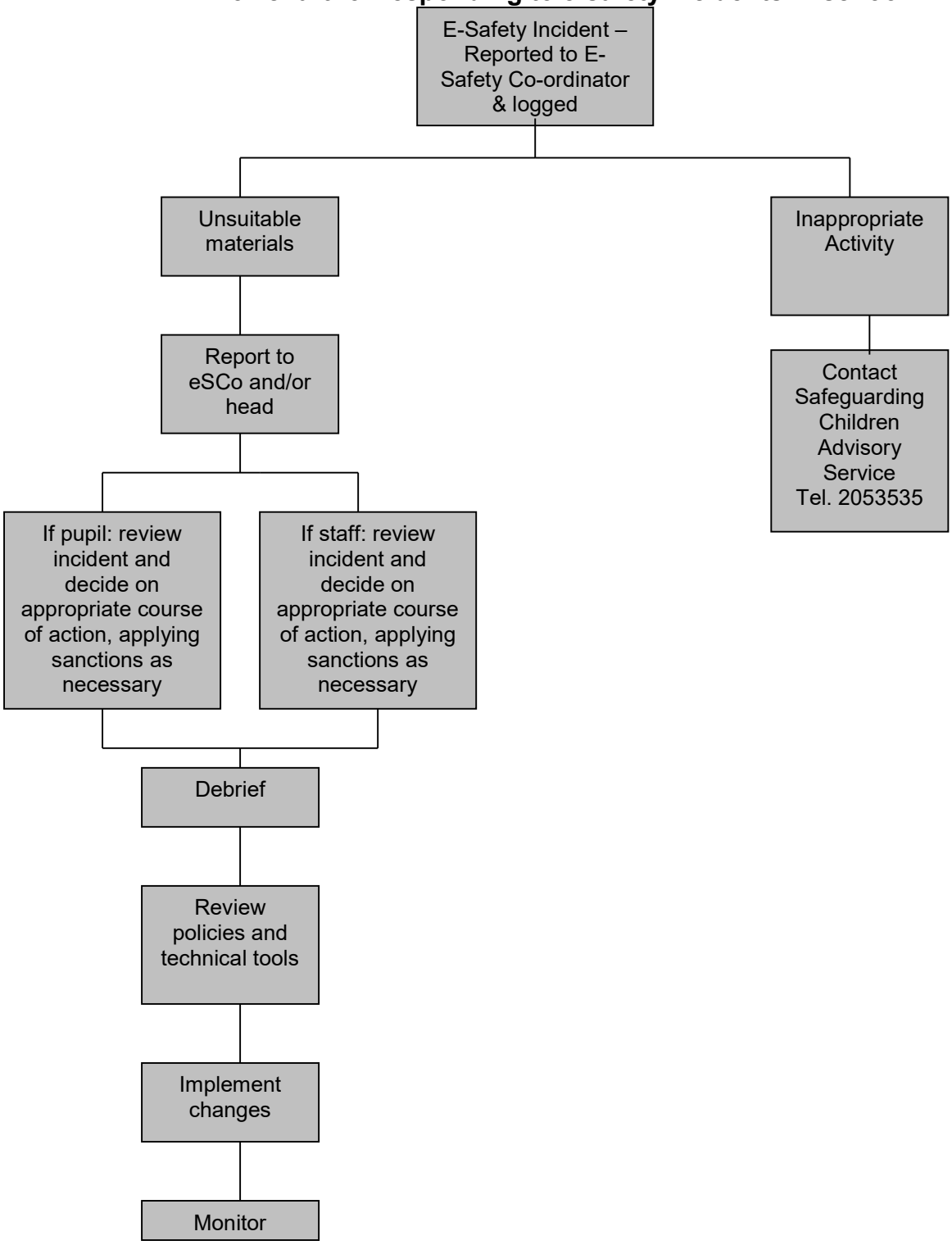
Letter to parents – Appendix C

Staff Acceptable Use Policy – Appendix D

Pupils Acceptable Use Policy – Appendix E

Appendix A

Flowchart for responding to e-safety incidents in school



Adapted from Becta – E-safety 2005

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

.

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 unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Our School

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 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

Appendix D

Staff and Volunteer Acceptable Use Policy

To ensure that staff and volunteers will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use. To ensure that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. The school will try to ensure that there is good access to ICT to enhance work and learning opportunities for all. We expect staff and volunteers to agree to be responsible users. Staff should consult the school's e-safety policy for further information and clarification.

For my professional and personal safety:

- 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 rôle.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- 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 rôle.
- 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.
- I will be professional in my communications and actions when using school ICT systems:
- I will not access, copy remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the schools policy on the use of

digital/video images. I will not use my personal equipment to record these images. If these images are published it will not be possible to identify subjects unless this has been sanctioned.

- I will not use any chat or social networking sites in school that are on the banned list.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will not be ′Friends′ with students or parents on social networking sites and I will follow school′s guidance on the use of such sites.

The school and the LA have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not use my mobile phone on the school premises whilst children are on the premises.
- If I use my personal email address on the school ICT systems I will ensure that such use is appropriate.
- I will not open any attachments to emails unless the source is known and trusted, due to the risk of the attachment containing viruses.
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal or inappropriate.
- I will only transport, hold, disclose or share personal information about myself or others as outlined in the School/LA Personal Data Policy. Where persoanl data is transferred outside the secure school network, I understand that it must be encrypted.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of School ICT systems out of school.

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 unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Any use of our school system implies agreement with this policy.

I have read, understood and agree with the Staff and Volunteer Acceptable Use Policy

Signed: …… Capitals: ……. Date: ……

Accepted for school: …… Capitals: ……

Please sign and return to the school office.

Pupils Acceptable Use Policy

- I will only use the school ICT equipment for purposes I have agreed with a member of staff
- I will keep my password and login private
- I will not interfere with anyone else's passwords, logins settings or files on the computer
- I will always seek permission before downloading material from the internet or using material I have brought into school because I understand the risks from virus infections
- I understand that I should only publish material on the internet that is my own work
- I know I need permission to take someone's photograph or video them
- Any messages I post on the Learning Platform or send in an email will be polite and responsible
- I will not send or forward messages or create material which is deliberately intended to cause upset to other people
- I will inform an adult if I see or receive any unpleasant material or messages
- I know I must take care about giving away my personal information and making contact with people I do not know using the internet
- I understand that the school may check my use of ICT and contact my parent/carer if they are concerned about my eSafety
- I understand that if I do not follow these rules I may not be allowed to use the school computers or access the internet for a period of time and that this may apply even if the activity was done outside school.

Pupil name.....

Signed.....

Date……..