Carfield Primary School E-Safety Policy

E-Safety Policy

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, Bullying, Curriculum, Data Protection, Social Networking and Security.

End to End e-Safety

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 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.

E-Safety Audit

Has the school an e-Safety Policy that complies with CYPD guidance?	Y
Date of latest update: June 2015	
The Policy was agreed by governors in 2010	
The Policy is available for staff on the S-Drive and web-site	
And for parents on the school's web-site	
The designated child protection officer is Adrian Digby	
The e-Safety Coordinator is Adrian Digby	
Has e-safety training been provided for both pupils and staff?	Y (KS2 not KS1)
Is the Think U Know training used?	Y
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 has been approved by SLT?	Y
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y

Contents

Carfield School e-Safety Policy

The e-Safety co-ordinator is Adrian Digby. The designated Child Protection Officer is Julie Petty. The designated Deputy Child Protection Officer is Carolyn Wilson. The learning mentor is Kay Johnson.

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 leadership team and approved by governors.

The e-Safety Policy will be reviewed annually. This policy will next be reviewed December 2013.

Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote student 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 students who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Students 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 students world-wide;
- access to experts in many fields for students 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 will be designed expressly for student use and includes filtering appropriate to students between the ages of 3 and 11.
- Students 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 students in on-line activities that will support learning outcomes planned for the students' age and maturity.
- Students 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 students who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. Staff only need to do this once.
- Parents will be informed that students will be provided with supervised Internet access.
- Parents and students will be asked to sign and return a consent form for student access.
- The Internet is available for use by all staff and students to access information to support the curriculum.
- Staff will receive training on the use of the Internet during school professional development days and after school sessions.
- Material published on the Internet is the responsibility of the staff member using the Internet or supervising students publishing work on the Internet. For this reason, no student material is to be published on the Internet without the permission of the supervising teacher and the child's parent/caregivers.
- Students will be given training in the use of the Internet as part of the ICT curriculum.
- Students will be allowed to use the Internet for a specific teacher authorised purpose under the supervision of a teacher.
- Students who inadvertently access an unfavourable site (including chat lines) must immediately inform the teacher.
- Students will not access the Internet without a teacher being present in the room.
- Students not to provide personal/school details on the Internet.
- Violations of any of the above will result in Internet access being revoked.

World Wide Web

- If staff or students 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 students and staff complies with copyright law.
- Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Students may only use approved e-mail accounts on the school system – since April 2010, these accounts have been accessible through Purple Mash (all students) and Sharp System (Y5/6).
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e- mail communication, or arrange to meet anyone without specific permission.
- Whole school/group or Purple Mash e-mail addresses only 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.

Cyber-bullying

- There are many types of cyber-bullying. The most common are detailed below. This list in not exhaustive and may become longer as new technologies and new threats emerge.
- Text messages —that are threatening or cause discomfort - also included here is "Bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology)
- Picture/video-clips via mobile phone cameras - images sent to others to make the victim feel threatened or embarrassed.
- Mobile phone calls — silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible. Emails — threatening or bullying emails, often sent using a pseudonym or somebody else's name.
- Chatroom bullying — menacing or upsetting responses to children or young people when they are in web-based Chatroom.
- Instant messaging (IM) — unpleasant messages sent while children conduct real-time conversations online using MSM (Microsoft Messenger) or Yahoo Chat – although there are others.
- Bullying via websites — use of defamatory blogs (web logs), personal websites and online personal "own web space" sites such as Bebo (which works by signing on in one's school, therefore making it easy to find a victim) and Myspace – although there are others.
- Students are encouraged to report any problems with cyber bullying to parents, teachers or other trusted adults (police if persistent and serious). They are informed that any type of bullying is not their fault, it can be stopped and usually can be traced.
- All incidents of cyberbullying will be dealt with at school in accordance with the school's anti-bullying policy
- To combat cyberbullying, students are encouraged to do the following: keep personal information secret and not post it on-line, keep and save any bullying emails, text messages or images as evidence; never reply to abusive emails, phone calls or text messages
- Serious bullying will be reported to the police - for example threats of a physical or sexual nature.
- Students should be made aware of their responsibilities to others, to respect other people - online and off, not to spread rumours about people or share their personal information, including their phone numbers and passwords.

Mobile Phone Use

- Children are generally not permitted to bring in or use mobile phones in school, on trips or on residentials
- If a parent has requested that a child bring a mobile phone into school, then the phone must be given to the class teacher, Deputy Headteacher, Headteacher or office at the beginning of the day. The phone will be returned at the end of the school day. Parents must agree that the school is not liable for any damage to or theft of the phone.
- If children have been requested by a teacher to bring their

mobile phones into school, e.g. for an ICT project, then the E-safety co-ordinator, Adrian Digby, must be informed; permission must be sought from parents and a separate risk assessment must be completed by the class teacher.

Social Networking

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

Gaming

- Many students are involved in online gaming at home
- Students should be made aware of age restrictions of online games
- Students should be made aware of the risks of playing games online with other people, especially people they don't know. These risks are very similar to those involved with chat-rooms and social-networking sites.
- Normally gaming sites would not be accessible in school, but educational games on sites such as the BBC may be used under teacher supervision.

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.

Video Conferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the students' 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.
- Staff will be issued with a school phone where contact with students 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 students personal information will not be published.
- The deputy headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' 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 students are published on the school Web site.
- Work can only be published with the permission of the student 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. For more information, see Data Protection Policy.

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. This e-safety policy is a working document and will be updated regularly as new technologies and new risks present themselves.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by the headteacher or deputy headteacher.
- 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.
- Students 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

Students

- Rules for Internet access will be posted in all networked rooms.
- Students will be informed that Internet use will be monitored.
- Students will be kept up-to-date with e-safety issues through regular e-safety assemblies – to be held termly for both KS1 and KS2 students
- There will be a special assembly and work done on Safer Internet Day (in conjunction with CEOP)
- Students will be informed of the SMART rules for Internet access.
- All Year 5 and Year 6 students will be educated in the use of the SHARP System.

Staff

- All staff will be given the School e-Safety Policy and its importance explained.
- All staff will be required to sign the Acceptable ICT Use Agreement, following the above.
- 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.
- Parents will be informed of any change to the e-safety policy.
- Parents will be informed of any introduction of new electronic systems, e.g. learning platforms and new technologies in school, through letters and dedicated parents' evenings.
- E-Safety evenings will be held annually, for parents. These will be delivered in conjunction with the LA and possibly other local schools.

Referral Process – Appendix A

E-Safety Rules– Appendix B

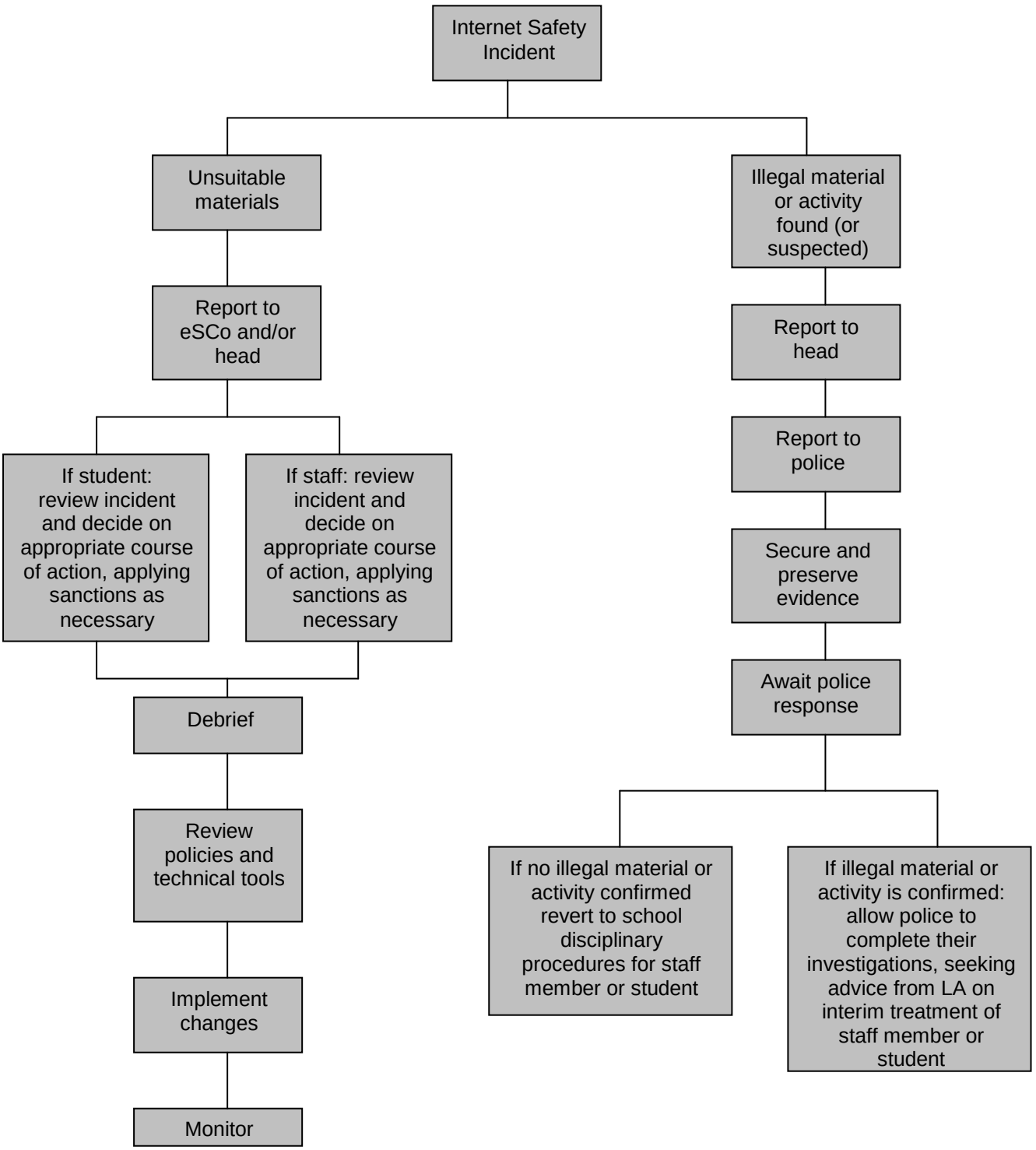
Letter to parents – Appendix C

SMART rules – Appendix D

Staff Acceptable Use Policy – Appendix E

Appendix A

Flowchart for responding to Internet safety incidents in school



Taken from Becta – E-safety 2005

Key Stage 1

Think then Click

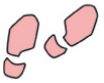
These rules help us to stay safe on the Internet

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

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

These e-Safety Rules help to protect students 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 authorised 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 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.

Edit this poster for display near computers.

Carfield Primary School

e-Safety Rules

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

Student's name:	***Class:***

Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	***Date:***

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 students 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 office.

Staff Information Systems Code of Conduct

- To ensure that staff 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 e-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 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 role.
- I will promote e-safety with students 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 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.

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

Signed: ……..…… Print name: ……..……

Date: …..……

Accepted for school: ……. Print name: …….

Follow the S.M.A.R.T. Rules

SAFE

Keep safe by being careful not to give out personal information – such as your name, email, phone number, home address, or school name – to people who you don't trust online.

MEETING

Meeting somebody you have only been in touch with online can be dangerous. Only do so
with your parents' or carers' permission and even then ONLY when they are present.

ACCEPTING

Accepting emails, instant messages or texts from people you don't know or trust can lead to
problems—they may contain viruses or nasty messages!

RELIABLE

Someone online may be lying about who they are, and information you find on the internet may not be reliable.

TELL

Tell your parent, carer or a trusted adult if someone or something makes you feel
uncomfortable or worried.

A. Digby - September 2010
Revised September 2011
September 2012
December 2012
January 2014
January 2015
June 2015