Seven Hills
School

Online Safety Policy

Agreed by governors: June 2014
Reviewed and amended: February 2016
Reviewed and amended: February 2018
Reviewed and amended: February 2020

Online Safety Policy

Overview

This policy was reviewed and revised in February 2018 and subsequently shared with staff, students, parents & governors.

Introduction

The purpose of information and communication technologies (ICT) 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.

Computing 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.
The Online Safety Policy addresses all safeguarding issues which relate to the use of ICT. There are two main elements to these issues:

1. Security: Procedures to protect the physical network infrastructure (to ensure the security of information including electronic data)
2. Online Safety: Procedures to ensure all members of the school community know their access rights and responsibilities in using ICT as summarized by the school's policies for reporting online safety incidents, Remote Access and Acceptable Use – see Appendices A to F)

Rationale

Rapidly developing information and communication technologies are exciting and motivating learning tools though which teaching and learning can be greatly enhanced. There are particular gains for students with SEN such as access to a broader community not limited by physical boundaries and support to communicate effectively through digital media. However those benefits must be balanced with an awareness of the potential risks. Seven Hills e-Safeguarding policy reflects our school's commitment to the safeguarding and well-being of our pupils through developing appropriate skills and awareness for staff and pupils to keep them safe in a technologically rich world. In terms of Data Protection, the school adheres to the principals of GDPR (General Data Protection Regulations) and has appointed to data protection officer to ensure the school complies with this legislation.

Roles and Responsibilities

Responsibilities of the School Community

We believe that online safety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Leadership Team

Develop and promote an online safety culture within the school community.

- Identify and support the e-safeguarding coordinator in their work.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to online safety effectively.
- Receive and regularly review online safety incident logs and be aware of the procedure to be followed should an online safety incident occur in school.
- Take ultimate responsibility for the online safety of the school community.

Responsibilities of the Online Safety **Coordinator** (C Rockliff)

- Promote an awareness and commitment to online safety throughout the school.
- Be the first point of contact in school on all online safety matters.
- Create and maintain online safety policies and procedures.
- Develop an understanding of current online safety issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in online safety issues
- Ensure that online safety education is embedded across the curriculum.
- Ensure that online safety is promoted with parents and carers.
- Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
- Ensure all staff know the correct reporting procedure should they feel they have an issue to report
- Monitor and report on online safety issues to Leadership Team and Governors as appropriate
- Ensure an online safety incident log is kept up-to-date.

Responsibilities of the Information Risk Officer (IRO)

- Be familiar with the risks associated with information held electronically within the school's infrastructure
- Ensure that information and data are stored and destroyed in line with the protocols and timescales set out in the GDPR.
- Know who has access to information within each level of classification (Information Asset Owners, IAOs) and why, keep an up to date retention schedule for all information data.
- Ensure that IAOs are aware of the restrictions concerning the information they handle
- Ensure information is retained and disposed of safely.
- Support in-service training on GDPR.
- Control and authorize access to information in consultation with the Online Safety officer

Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school's Online Safety policy and guidance.
- Read, understand and adhere to the school staff Acceptable Use Policy and in particular those referring to Remote Access (Appendices E and F)
- Develop and maintain an awareness of current online safety issues and guidance.
- Model safe and responsible behaviours in your own use of technology.
- Embed online safety messages in learning activities where appropriate.
- Supervise pupils carefully when engaged in learning activities involving technology.
- Be aware of what to do if an online safety incident occurs.
- Maintain a professional level of conduct in your personal use of technology at all times.

Responsibilities of Technical Staff

- Read, understand, contribute to and help promote the school's online safety policy and guidance.
- Read, understand and adhere to the school staff Acceptable Use Policy
- Support the school in providing a safe technical infrastructure to support learning and teaching; specifically:
    - Where any external network traffic is allowed from the Internet to the school, a local firewall(Smoothwall) shall be deployed to restrict traffic into only necessary ports and IP addresses
    - All Internet-facing systems shall be placed onto a separate network segment; a de-militarised zone (DMZ) with access to applicable services, controlled by a firewall

  - All wireless implementations shall be encrypted, and shall require authentication prior to connection
- Take responsibility for the security of the school ICT system, specifically:
  - All externally facing devices shall be hardened and patched to ensure no high-risk vulnerabilities are present
  - All desktops shall have up-to-date anti-malware software installed
  - All incoming e-mail shall be scanned for malware and filtered for spam – via Gmail system.
  - All anti-malware software (currently SOPHOS) shall be configured to alert the ICT Technicians when any malware is detected.
  - All malware definitions should be updated daily
  - All pupil access to the internet should be filtered for inappropriate use
  - All hard discs, and any other media containing school information (including backup media) shall be securely deleted, either by specialist deletion utilities or physical destruction prior to disposal.
  - Data backups are automated, taken at regular intervals (daily) and backup media should be kept at different location to main servers.
  - Use a log consolidation tool in conjunction with a network time protocol server to enable accurate analysis of logs.
- Report any online safety -related issues that come to your attention to the online safety co-ordinator. Daily Smoothwall reports are automatically generated and sent to the Online Safety Coordinator. The ICT Technicians provide a monthly summary report.
- Develop and maintain an awareness of current online safeguarding issues, legislation and guidance relevant to your work.
- Liaise with the local authority and others on technical issues.
- Maintain a professional level of conduct in your personal use of technology at all times.

Responsibilities of Pupils

- Read and/or understand and adhere to the school pupil Acceptable Use Policy.
- Help and support the school in creating e-safeguarding policies and practices; and adhere to any policies and practices the school creates.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
- Take responsibility for your own and each others' safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside of school. Accept responsibility for your comments made on social networking sites and/or text messages sent
- Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
- Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone who this is happening to.
- Discuss online safety issues with family and friends in an open and honest way.

- **Responsibilities of Parents and Carers**
- Help and support your school in promoting online safety.
- Read, understand and promote the school pupil Acceptable Use Policy with your children.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.

- Take responsibility for your own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Discuss online safety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in your own use of technology.
- Accept responsibility for your son/daughter's comments made on social networking sites and/or text messages sent
- Ensure that you monitor your son/daughter's use of the internet at home
- Consult with the school if you have any concerns about your child's use of technology.

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's online safety policies and guidance.
- Develop an overview of the benefits and risks of the Internet and common technologies used by pupils.
- Develop an overview of how the school ICT infrastructure provides safe access to the Internet.
- Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in e-safeguarding activities.
- Ensure appropriate funding and resources are available for the school to implement their e-safeguarding strategy.

Approach/ Policy Content

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the Internet brings.

- We will provide online safety as an integral part of lessons taught in Computing / PSHE for all year groups as appropriate to need.
- We will celebrate and promote online safety through a planned programme of assemblies and whole-school activities.
- We will discuss, remind or raise relevant online safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
- We will continue to research and make use of a range of available resources, including those produced by CEOP, UK Safer Internet Centre, Childnet & National Education Network
- We will remind pupils about their responsibilities through an end-user Acceptable Use Policy which all appropriate pupils will sign. This will also be displayed throughout the school, along with Internet Safety rules.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

How Parents and Carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

- hold annual parent meetings/ events on online safety

- include useful links and advice on online safety on our school website
- provide parents/carers with fact sheets from CEOP about online safety
- include a section on online safety in the School Information Booklet.

Managing ICT Systems and Access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.
- The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.
- All users will sign an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.
- Secondary pupils will access the Internet using an individual log-on, which they will keep secure. Whether supervised by a member of staff, or working independently, pupils will abide by the school AUP at all times.
- Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the school AUP at all times.
- Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff, e.g. head teacher and member of technical support.
- Access to the wireless network will be set so that unauthorised users nearby cannot inadvertently or deliberately connect.
- The installation of any software or hardware on school ICT systems without permission is forbidden.
- In the event of a request to the ICT technicians to unblock an internet site, the Head Teacher/ school Online Safety Coordinator will be notified of the web address and reason for the request.
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur.
- The school will regularly audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimize risks.

Filtering Internet Access

- The school uses a filtered Internet service. The filtering is provided through - Smoothwall web filtering
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the online safety coordinator.
- If users discover a website with potentially illegal content, this should be reported immediately to the online safety coordinator. The school will report this to appropriate agencies including the filtering provider, LA, CEOP or IWF.
- The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

Learning Technologies in School

	Pupils	Staff
Use of blogs, wikis, podcasts	allowed with supervision. Blogs only within VLE	allowed
social networking sites	not allowed	not allowed
Use of video conferencing or other online video meetings	allowed with supervision	allowed
Personal mobile phones brought into school	allowed	allowed
Mobile phones used in lessons	not allowed	school phones only and for curriculum purposes only
Mobile phones used outside of lessons	allowed only with permission	Allowed, but not in front of students
Taking photographs or videos on personal equipment	not allowed	not allowed
Taking photographs or videos on school devices	allowed with supervision	allowed
Use of hand-held devices such as MP3 players or personal gaming consoles	allowed at certain times	allowed at certain times
Use of personal email addresses in school	not allowed	allowed with specific permission from Head teacher
Use of school email address for personal correspondence	not allowed	not allowed
Use of online chat rooms	not allowed	not allowed
Use of instant messaging services	not allowed	not allowed
Any other new technologies school wishes to consider	allowed with supervision	allowed following discussion with online safety coordinator/ risk assessment officer

Using Email

- Staff and pupils should use approved e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system will be monitored and checked.
- Students will be provided with log in details for using Purple Mash and supported to use the messaging facility as appropriate.
- Pupils will be reminded when using messaging systems about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening messages/e-mails from an unknown sender, or viewing/opening attachments.
- Pupils are not permitted to access personal e-mail accounts during school.
- Staff may only access personal email in school following specific permission from the Head teacher.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only. This should be via school systems and never using a personal email address
- Any inappropriate use of the school e-mail system or other web-based systems, or the receipt of any inappropriate messages by a user, should be reported to a member of the leadership team immediately.

Using Images, Video and Sound

- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.

- Digital images, video and sound will only be created using equipment provided by the school.
- Staff and pupils will follow the school policy on creating, using and storing digital resources.
- In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources
    a. will not be published online without the permission of the staff/pupils involved.
    b. if pupils are involved, relevant parental permission will also be sought before resources are published online.

Using blogs, wikis, podcasts, and other ways for pupils to publish content online

- We may use blogs/wikis/podcasts /other ways to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.
- Blogging, podcasting and other publishing of online content by pupils will take place within the school learning platform. Pupils will not be allowed to post or create content on sites where members of the public have access.
- Any public blogs to be run by staff on behalf of the school will be hosted on the learning platform/school website and postings will be approved by the Headteacher before publishing.
- Pupils will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them. Pupils will not use their real name when creating such resources. They will be encouraged to create an appropriate 'nickname'.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside of school. If staff use social networking sites they should not communicate with students or their families, whilst they still attend Seven Hills, nor until they are 18 or over.

Using Video Conferencing and Other Online Video Meetings

We may use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. However, we will ensure that staff and pupils take part in these opportunities in a safe and responsible manner.

- All video conferencing activity will be supervised by a suitable member of staff.
- Pupils will not operate video conferencing equipment, or answer calls, without permission from the supervising member of staff.
- Video conferencing equipment will be switched off and secured when not in use
- Pupils will be given appropriate user rights when taking part in an online meeting room. They will not have host rights or the ability to create meeting rooms.
- Parental permission will be sought before taking part in video conferences.
- Permission will be sought from all participants before a video conference is recorded. Video conferences should only be recorded where there is a valid educational purpose for reviewing the recording. Such recordings will not be made available outside of the school.

Using Mobile Phones

- Personal mobile phones may not be used during lessons.
- Pupils will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be available. Staff should not use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil, parent or family.
- Mobile phones are a common vehicle for cyberbullying, through the recording of inappropriate images or video, distributing such images and videos via Bluetooth or other wireless technologies, or the sending of abusive text messages. Cyberbullying is specifically referred to within the school Anti-Bullying Policy.

New Technologies

- As a school we will keep up to date with new technologies and consider both the benefits for learning and teaching and also the risks from an online safety point of view.
- We will regularly amend the online safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an online safety risk.

Protecting Personal Data

- We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff will ensure they properly log-off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive data from the school premises without permission of the Head teacher, and without ensuring such data is kept secure through password protection/encryption.
- When e-mailing confidential information (even to members of staff within school) the information in question should be contained within a password-protected document. The password for the document should not be included in the email or email thread and should be communicated separately if required.

The School Website and Other Online Content Published by the School

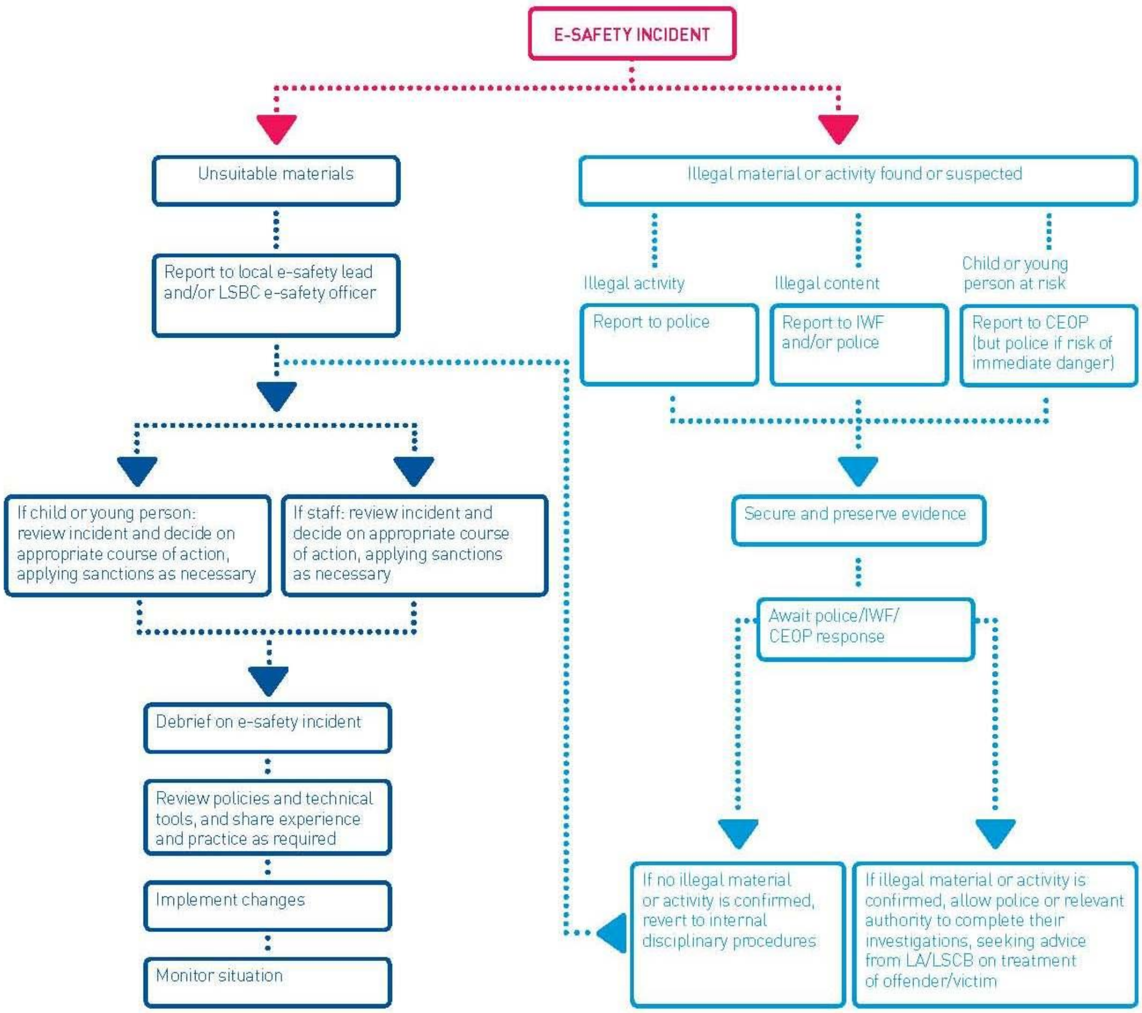
- The school website will not include the personal details, including individual e-mail addresses or full names, of staff or pupils.
- A generic contact e-mail address will be used for all enquiries received through the school website.
- All content included on the school website will be approved by the Head Teacher before publication.
- The content of the website will be composed in such a way that individual pupils cannot be clearly identified.
- Staff and pupils should not post school-related content on any external website without seeking permission first.

Appendix A – Dealing with online safety Incidents

Appendix B – Online Safety Rules
Appendix C – Safety Rules Poster
Appendix D – Letter to Parents/ Carers
Appendix E – Remote Access
Appendix F – Staff Acceptable Use Policy

Appendix A Flowchart for Responding to Online Safety Incidents

Flowchart for responding to e-safety incidents

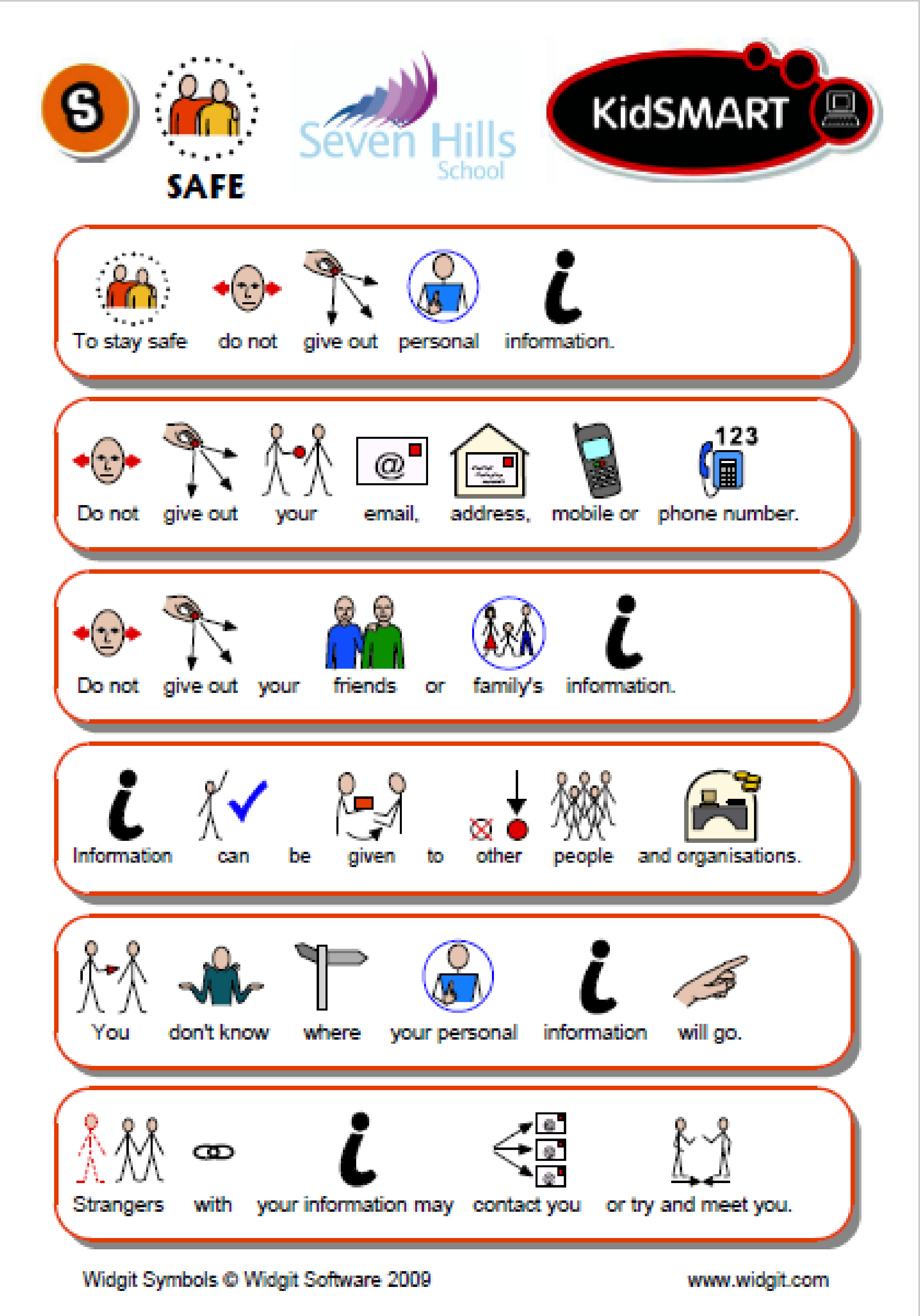

E-SAFETY INCIDENT
Unsuitable materials
Report to local e-safety lead and/or LSBC e-safety officer
If child or young person: review incident and decide on appropriate course of action, applying sanctions as necessary
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Debrief on e-safety incident
Review policies and technical tools, and share experience and practice as required
Implement changes
Monitor situation
Illegal material or activity found or suspected
Illegal activity
Illegal content
Child or young person at risk
Report to police
Report to IWF and/or police
Report to CEOP (but police if risk of immediate danger)
Secure and preserve evidence
Await police/IWF/ CEOP response
If no illegal material or activity is confirmed, revert to internal disciplinary procedures
If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from LA/LSCB on treatment of offender/victim

(reproduced from 'AUPs in Context: Establishing Safe and Responsible Online Behaviours', © copyright Becta 2009)

The LA Safeguarding Sheffield Children may be contacted for advice at all times on telephone: 0114 2053535, email: child.protection@sheffield.gov.uk

Appendix B

Online Safety Rules for Seven Hills School



SAFE

Seven Hills School

KidSMART

To stay safe do not give out personal information.

Do not give out your email, address, mobile or phone number.

Do not give out your friends or family's information.

Information can be given to other people and organisations.

You don't know where your personal information will go.

Strangers with your information may contact you or try and meet you.

Widgit Symbols © Widgit Software 2009 www.widgit.com

SAFE

Seven Hills School

KidSMART

Companies may want your personal information to sell you things.

You may be asked to register and fill in your personal information.

If you are unsure, ask an adult for advice.

Keep your blog and profiles private on social networking sites.

In chat areas you may be asked age, sex, location (ASL).

Don't tell anyone where you live and your full name.

Appendix C

Safety Rules

For display in each room where there are computers

These Online 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 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.

Appendix D **Letter to Parents/ Carers**

Seven Hills School

Online 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 Online Safety **Rules have been understood and agreed.**

Parent’s Consent for Web Publication of Work and Photographs

I ***agree/do not agree*** that my son/daughter’s work may be electronically published. I also ***agree/do not 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 online-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.

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 E **Remote Access** (Responsibility: All Staff)

The use of mobile computing devices and connecting to the school's network from home is increasingly important but presents a number of security risks. Users of mobile computing devices (such as laptops) are responsible for safeguarding such equipment and should take all responsible precautions to prevent theft, loss or damage of such items, and to prevent unauthorised access to information held on the device. Particular care should be taken when leaving devices in cars, hotel/holiday accommodation, or the home, ensuring they are not visible. Where possible, mobile devices should be locked away when not in use.

The following guidelines shall apply when accessing systems and information away from the school:

a) **Only necessary information should be stored on the device.**

b) **Pupil-sensitive (restricted) information shall not be stored on any mobile devices unless encrypted/password protected.**

c) **Work away from school, involving the access and use of sensitive (restricted) data, should be done via secure remote access technology and shall require a username and password to secure the personal data of learners, staff and other authorised users.**

d) **When working away from school via remote access technology, staff shall not save copies of restricted data onto their portable device.**

e) **All remote access attempts should be subject to account locking after a maximum of 5 failed attempts.**

The removal of any ICT equipment, information and software from school premises shall only be permitted with prior authorisation from the Network Manager or Head Teacher.

.

Appendix F Staff Acceptable Use Policy

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-safeguarding 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 I follow the guidelines covered in appendix E (Remote Access) when accessing systems and information away from the school.
- 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 /Designated Safeguarding Lead and log any incidents on CPOMS.
- I will ensure that any electronic communications with pupils are compatible with my professional role and will only use school e-mail addresses.
- If I request the unblocking of an internet site by the ICT technicians, I will notify the Head Teacher/school e-Safety Coordinator of the web address and reason for the request.
- 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 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 ……………………………… Name (capitals) ……………………….. Date ……………….

Accepted for school: …………………………… Name (Capitals): ………………………….