Heron Cross Primary

Edited from draft policy at:
www.sgfl.org.uk/e-safety

Heron Cross Primary

E-Safety Policy

Primary School Core Policy

Stoke-on-Trent Children and Young People's Services has approved this core e-Safety Policy which may be used by primary and special schools as the basis to construct their own policies.

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Any previous Internet policy should be revised and renamed as the school's e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection 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 Stoke-on-Trent Education WAN including the effective management of Websense filtering.
- National Education Network standards and specifications.

E-Safety Audit – Primary / Special

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place to support a range of activities that might include those detailed within Appendix 1.

Has the school an e-Safety Policy that complies with C&YP guidance?	Y
Date of latest update: Dec 2009	
The Policy was agreed by governors on:	
The Policy is available for staff at: Office	
And for parents at: to be published on web site	
The Designated Child Protection Coordinator is: D Shenton	
The e-Safety Coordinator is: S Chubb	
Has e-safety training been provided for staff?	Feb 2010
Has e-safety training been coherently planned and delivered for pupils?	Implemented spring/summer 2010
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
Have school e-Safety Rules been set with pupils?	Y
Are these Rules displayed in all rooms with computers?	ICT suite
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access (e.g. Stoke-on-Trent Educational WAN).	Y
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y
Do all school computers have e-safety text monitoring software (Forensic) installed?	Y

School e-safety policy

2.1 Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, Bullying and for Child Protection.

- The school will appoint an e-Safety Coordinator. This was appointed on Feb 2009 as being S Chubb.
- Our e-Safety Policy has been written by the school, building on the Stoke-on-Trent e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors and the PTA.
- The e-Safety Policy and its implementation will be reviewed as needed.
- The e-Safety Policy was revised by: S Chubb
- It was approved by the Governors on: … … ……..

2.2 Teaching and learning

2.2.1 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Staff will vet website before sharing with pupils.
- Pupils will be educated in the effective use of the Internet in research, including the skills of effective knowledge location, retrieval and evaluation.

2.2.2 Pupils will be taught how to evaluate Internet content

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2.2.3 Pupils will be taught how to stay e-safe

- Curriculum planning will include age appropriate opportunities to discuss, role play and learn about the benefits and risks offered by new technologies, such as e-mail, mobile phones and social networking sites.
- E-safety delivery will be mapped across the curriculum to ensure full coverage.

2.3 Managing Internet Access

2.3.1 Information system security

- Virus protection will be updated regularly on all networked computers.
- School ICT systems capacity and security will be reviewed regularly.

2.3.2 E-mail

- 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.
- The forwarding of chain letters will be banned.

2.3.3 Public Web published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The ICT coordinator will take overhaul editorial responsibility and ensure that content is accurate and appropriate, with final editorial decisions being under the direction of the Head teacher.
- The website will comply with the school's guidelines for publications, including respect for intellectual property rights and copyright.

2.3.4 Web Publishing pupils' images and work

- Images, published to the web, that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published to the web.

2.3.5 Social networking and personal publishing

- The City Council/school will block/filter access to social networking sites, except those specifically purposed to support educationally approved practice.
- Newsgroups will be blocked unless a specific use is approved.
- Staff and pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Staff and pupils should be advised not to publish specific and detailed private thoughts on social networking sites.

2.3.6 Managing filtering

- The school will work with Stoke-on-Trent City Council, Becta and the WAN Managed Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, the URL must be reported to the ICT coordinator or Head teacher. The ICT coordindator or Technician will ensure the site is reported on the "Report Abuse" facility in SCORE.
- The technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.3.7 Managing remote teaching/video-conferencing

The equipment and network

- Full IP videoconferencing will use the national educational or the schools' broadband network to ensure quality of service and security.
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact information will not be put on the school Website.
- School videoconferencing equipment will not be taken off school premises without permission, since use over a non-educational network (e.g. the internet) cannot be monitored or controlled.

Users

- Pupils will ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be supervised appropriately for the pupils' age.
- Parents and guardians will agree for their children to take part in videoconferences, probably in the annual return.
- Responsibility for the use of the videoconferencing equipment outside school time will be established with care.
- Only key administrators will be given access to the videoconferencing system, web or other remote control page available on larger systems.
- Unique log on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission will be sought by all sites and participants. The reason for the recording is given and the recording of videoconference is clear to all parties at the start of the conference.
- Recorded material will be stored securely.
- If third-party materials are to be included, recordings will be checked that they are acceptable to avoid infringing the third party intellectual property rights.
- Dialogue will be established with other conference participants before taking part in a videoconference. If it is a non school site it is checked that they are delivering material that is appropriate for the class.

2.3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out and protocols established before use in school is allowed.
- Mobile phones will allowed during formal school time, unless specifically allowed to support learning as identified by the teacher. The sending of abusive or inappropriate text messages is forbidden, and children will be taught strategies to deal with inappropriate texts or picture messages.

- Staff will be issued with a school phone where text or mobile contact with pupils is required.

2.3.9 Protecting personal data

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

2.4 Policy Decisions

2.4.1 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications, which includes internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.
- At Key Stage 1 access to the Internet will be by adult demonstration or by directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Sanctions for inappropriate use will be drawn up and shared with staff and pupils.

2.4.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Stoke-on-Trent City Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

2.4.3 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.

2.4.4 Community use of the Internet

- The school learning platform will be made accessible to the community with an interest in the school. Users will be permitted access which is appropriate, whilst ensuring child protection issues are not compromised.

2.4.5 Cyberbullying – Understanding and Addressing the issues

While cyberbullying is likely to be low level in primary schools the age of pupils making proficient use of technology is ever decreasing. Therefore, the opportunities for pupils to bully or be bullied via technology, such as e-mail, texts or MSN, are becoming more frequent.

As such, teaching pupils about appropriate behaviours when using technology provides a vital grounding for future use and will be taught in all year groups above year2. Whilst not wanting to provoke unrecognised opportunities in pupils, consideration must be given to suitable teaching and procedures to address any issues of cyberbullying.

As felt appropriate for the age and use of technology by the pupils:

- The school's anti-bullying policy and/or school behaviour policy will address cyberbullying. Cyberbullying will also be addressed in ICT, PHSE and other relevant lessons and is brought to life through activities. As with other whole-school policies, all staff and young people will be included and empowered to take part in the process.
- Pupils, parents, staff and governors will all be made aware of the consequences of cyberbullying. Young people and their parents will be made aware of pupils' rights and responsibilities in their use of new technologies, and what the sanctions are for misuse.

2.4.6 Cyberbullying - How will risks be assessed?

- The school will take all reasonable precautions to ensure against cyberbullying whilst pupils are in its care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a school computer will not occur. Neither the school, nor Stoke-on-Trent City Council, can accept liability for inappropriate use, or any consequences resulting outside of school.
- The school will proactively engage with KS2 pupils in preventing cyberbullying by:
    - understanding and talking about cyberbullying, e.g. inappropriate use of e-mail, text messages;
    - keeping existing policies and practices up-to-date with new technologies;
    - ensuring easy and comfortable procedures for reporting;
    - promoting the positive use of technology;
    - evaluating the impact of prevention activities.
- Records of any incidents of cyberbullying will be kept and will be used to help to monitor the effectiveness of the school's prevention activities.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

2.4.7 How will cyberbullying reports/issues be handled?

- Complaints of cyberbullying will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Evidence of offending messages, pictures or online conversations will be kept, in order to demonstrate to others what is happening. It can be used by the school, internet service provider, mobile phone company, or the police, to investigate the cyberbullying.

- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions within the school discipline policy include:
    - interview/counselling by the class teacher;
    - informing parents or carers;
    - removal of Internet/computer access for a period or banning of mobile phone in school.

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with pupils at the start of each year and as the need arises.
- Pupils will be informed that network and Internet use will be monitored.

- An e-Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- An e-Safety module will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.

2.5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its application and importance explained.
- All staff will be informed that all computer and Internet use will be monitored. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

2.5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure, on the school website and through parents' sessions.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Networked favourites Ikeepbookmarks.com SCORE minisites
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. ▪ Ask Jeeves for kids ▪ Yahooligans ▪ CBBC Search ▪ Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	SCORE sgfl accounts School Net Global E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites for feedback.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils should be encouraged to report any inappropriate comments.	SCORE Showcase Making the News Podcasts
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within blogs, chat rooms or online forums.	Only blogs/chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SCORE Blogs SuperClubs Skype FlashMeeting Cyber Cafe
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype FlashMeeting National Archives "On-Line" Global Leap National History Museum Imperial War Museum

Dated : March 2014 Signed: Headteacher.....

Review Date: March 2015 Signed: Chair of Governors .....