Policy for E-Safety

Helmingham Community Primary School

Written by: Charlotte Salmon

Date: October 2015

Approved by: ……..

Date of approval: ……...

To be reviewed October 2016

Helmingham Community Primary School
E-Safety Policy

Aim

The aim of this policy is to ensure that the whole school community, adults and children are aware of the safety issues associated with information systems and electronic communications. Its purpose is to allow all members of our community to enjoy the many benefits of electronic communications whilst understanding the dangers and taking appropriate precautions to keep themselves safe.

What is E-Safety?

E-Safety encompasses Internet technologies and electronic communications such as mobile phones. This policy supports the education of children about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences. This policy will operate in conjunction with other school policies including those for Computing, Behaviour, Bullying, PSHE, Safeguarding and Acceptable Use Policy (AUP). The school's E-Safety Co-ordinator is Mrs Salmon, who will work closely with the Senior Designated Professionals for Safeguarding, Mrs Cleland.

E-Safety is achieved through the responsible use of IT by all staff and children; sound implementation of e-safety policy in both administration and curriculum, including a safe and secure broadband from the Local Authority including the effective management of content filtering.

Essentials in Place

- Firewalls provided by AVG
- Anti-virus and anti-spyware software provided by AVG
- Filters provided by E2BN
- Using an accredited IS - E2BN LA provider
- Awareness of wireless technology issues - monitored termly by Gill Davidson, our Technical Software Support for optimum performance and safety
- A clear policy on using personal devices - part of this policy

Teaching and Learning

- 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 functions.
- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- Children use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- At Key Stage 1 children's access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 2 children will be supervised by teachers and teaching assistants when using the Internet. Children will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

Benefits of Using the Internet in Education

- Access to worldwide educational resources including Catch-Up, Purple Mash, RM Maths and many others, are a platform for showing our work;
- Educational and cultural exchanges between children worldwide;
- Access to experts in many fields for children and staff;
- Professional development for staff, educational materials and effective curriculum practice;
- Collaboration across networks of schools, 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.

Using the Internet to Enhance Learning (schools overview for e-safety planning in *Appendix 1*)

- The school's Internet access has been designed to enhance and extend education.
- Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of children.
- Staff will guide children in online activities that will support the learning outcomes planned for the children's age and ability.
- Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Children will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Information Systems

- Personal data sent over the Internet or taken off site will be encrypted.
- Virus protection will be updated regularly.
- Portable media can be used following an anti-virus /malware scan.
- Files held on the school's network will be regularly checked and backed up to the server daily.
- The server will be backed up and the external hard drive kept in the school library that is locked and alarmed out of school hours.
- The use of user logins and passwords to access the school network will be enforced.

Email (Children's own email accounts not applicable as yet, once set up in the future this will apply)

- Children may only use approved email accounts for school purposes as provided by Local Authority or other vetted provider.
- Children must immediately tell a teacher if they receive offensive emails.
- Children must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole-class or group email addresses will be used in school for communication outside of the school.
- Access in school to external personal email accounts may be blocked.
- Emails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Staff will not use personal email accounts whilst teaching or for professional purposes.

Published Content and School Web Site

- The contact details on the website should be the school address, email and telephone number. Staff or children's personal information will not be published.
- The head teacher will take overall editorial responsibility and will ensure that content published is accurate and appropriate.
- Parents give permission or not for the use of photographic images of children to be used by the school when enrolling their children.
- Children's full names will not be used anywhere on the website, particularly in association with photographs.

Social Networking (See additional guidance on the use of social networking and social media sites in *Appendix* 2)

- The school will block/filter access to social media and social networking sites.
- Children will be advised never to give out personal details of any kind which may identify them and/or their location.
- Children will be advised not to use personal photos on any social network sites.
- Children will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals, block unwanted communications. Children will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful ordefamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy. This includes not accepting requests from students on social websites.

Filtering

- The school will work with the Local Authority, E2BN and the Schools Broadband team to ensure that filtering systems are as effective as possible.

Video Conferencing

- Video conferencing will be supervised by a member of staff.
- Staff will check and establish dialogue with other conference participants before taking part in a video conference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.
- IP video conferencing will use educational broadband network to ensure quality of service and security rather than the Internet.

Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Children will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Policy.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Usernames and passwords are used to keep data secure.

Risk Assessment

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school undertakes regular audits of ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. Please see *Appendix 3* of our schools audit.

Responding to Incidents

- Complaints of Internet misuse by children will be dealt with by the class teacher in the first instance. Serious instances of misuse will be dealt with by the Headteacher or Senior Teacher.
- Any complaints of staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with our school safeguarding policy.

Cyber Bullying

- Children will be taught about the effects of cyber bullying and how to report cyber bullying through PSHE lessons and specially arranged workshops (*Appendix 1*).
- Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- All incidents of cyber bullying reported to the school will be recorded and investigated by the Headteacher.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Mobile Phones and Personal Devices

- Mobile phones and personal devices are not permitted to be brought on to the school site by the children. Staff will turn their phones off/to silent on entering the school premises and are not to be used during the working day or as a recording device on school trips.

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- The school will provide a school mobile phone for emergency contact only by school staff. The schools mobile phone can be taken on school trips.

Children Use of Personal Devices

- If a child breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during the working day unless permission has been given by Headteacher or Senior Teacher in emergency circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action will be taken.

Communication Policy

- All users will be informed that network and Internet use will be monitored.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An E-Safety module will be included in the PSHE, Citizenship and/or Computing programmes covering both safe school and home use.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

Staff

- The E-Safety Policy will be formally provided to and discussed with, all members of staff through a yearly staff meeting.
- An e-safety audit (*Appendix 3*) will be carried out regularly by the E-Safety Co-ordinator to assess whether the e-safety basics are in place.
- To protect all staff and children, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All staff will have access to e-safety contacts and references (*Appendix 4*).

Parents

- A partnership approach to e-safety at home and at school with parents will be encouraged. This may include offering parent evenings or workshops with demonstrations and suggestions for safe home Internet use, or highlighting E-Safety at other attended events e.g. parent evenings, open days, home and school communication booklets, access to the e-safety policy through the schools website.
- Information and guidance for parents on e-safety will be made available to parents in a variety of formats.

The E-Safety Policy and its implementation will be reviewed annually.