Hinchley Wood Primary School
E-safety Policy

Writing and reviewing the E-safety policy

Children's safety and well-being are a key part of our school aims and a focus of all of our work with the children. In this context, the E-safety Policy is part of the School Development Plan for 2016-19 and relates to other key policies including those for ICT, bullying and for child protection (ref. Behaviour and Safety Committee).

- **The school's E-safety coordinator is tbc.**
- Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by all staff and approved by governors.
- All staff are required to know the details of this policy and confirm this in writing annually. They will model safe practise, as set out in this policy at all times.
- The E-safety Policy and its implementation will be reviewed annually.

Teaching and learning

Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- **Internet use will enhance learning**
- The school Internet access is provided by RM and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school seeks to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are taught how to report unpleasant Internet content.
- For children with social, familial or psychological vulnerabilities, further consideration should be taken to reduce potential harm.

Managing Internet Access

Information system security

- School ICT system's security is reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

E-mail

- **Pupils and staff 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.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Neither staff or pupils' personal information will be published on the school website.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils must not place personal photos on any social network space provided in the school learning platform.
- Pupils and parents will be advised that the use of social network spaces outside school can present dangers for primary aged pupils.

- Pupils will be advised to use nicknames and avatars when using social networking sites

Managing filtering

- The school will work in partnership with Surrey County Council to ensure systems to protect pupils are reviewed regularly, and improved, as required.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-safety Coordinator (Computing subject leader).
- The Computing subject leader will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Videoconferencing will use the educational broadband network, rather than the internet, to ensure quality of service and security.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Mobile phones are not permitted for use by the children in the course of the school day.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- If a pupil breaches the school policy then the phone or device will be confiscated and held in the school office.
- Handheld technologies, including games and mobile phones, often have internet access which may not include filtering. Care will be taken with their use within the school.
- Staff will use a school phone where contact with pupils is required.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.

- **Protecting personal data**

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

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT ' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- In the EYFS, Key Stage 1 and 2, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site.

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 SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

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 head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Communications Policy

Introducing the E-safety policy to pupils

- Appropriate elements of the E-safety policy will be shared with pupils.
- E-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils

Staff and the E-safety policy

- All staff will be given the School E-safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential (ref. school code of conduct).
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on E-safety.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents who volunteer to help in school will be asked to read the policy and sign to confirm they have understood the contents.

Written by- S Evans & R Collomosse