E-safety policy

Policy Originator: Computing Leader **Review period: 3 years**

Governors' Committee Responsible: Children and Learning **Next Review: Autumn 2017**

The E-safety Policy relates to other policies including those for Computing, bullying, PSHE and for child protection.

- **The school has a designated E-safety Leader**
- Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors
- The E-safety Policy and its implementation will be reviewed annually
- The E-safety Policy was revised by: **Ben Viner (Computing Leader) on 21/9/14**

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 Computing experiences as part of their learning
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils
- The school Internet access is provided by Surrey County Council through the Unicorn contract and includes a new and highly effective filtering firewall (Smoothwall) thus creating a managed and customisable environment appropriate to the age of pupils
- Pupils are rigorously taught what Internet use is acceptable and what is not and are given clear objectives for all Internet use
- Pupils are educated in safe searching skills and how to assess the reliability of websites when using the Internet thus teaching them how to access safe and age appropriate digital resources
- Pupils are shown how to publish and present information appropriately to a wider audience
- Pupils are taught how to use online communication tools effectively and safely

Pupils will be taught how to evaluate Internet content

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law
- Where possible, pupils are encouraged to verify the information they find online with other sources, e.g. books
- Pupils will be taught how to report content that concerns them to a member of teaching staff

- Given the unfortunate rise in the profile of Cyber-bullying (the use of digital media to harass, threaten or intimidate individuals) children will be taught what it is, the consequences it can cause and what to do, should they fall victim to it, to report incidents.
- Staff have been trained in CEOPS reporting procedures and how to access ThinkuKnow resources to aid the teaching of Cyber-bullying and the safe use of the internet and other online devices.
- A CEOPS button has been added to the school website to facilitate reporting procedures

Pupils will be taught how to evaluate Internet content

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law
- Where possible, pupils are encouraged to verify the information they find online with other sources, e.g. books
- Pupils will be taught how to report content that concerns them to a member of teaching staff

Managing Internet Access

Information system security

- School ICT systems security is reviewed regularly
- Virus protection is updated regularly
- Security strategies are discussed with the Local Authority
- Remote access limits the transfer of information on flash drives

E-mail

- Staff may only use approved e-mail accounts on the school system
- Incoming e-mail where the author is unknown will be treated as suspicious and attachments not opened

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 pupils personal information will not be published
- The Head Teacher has overall editorial responsibility and ensures that content is accurate and appropriate

Publishing pupil's images and work

- Written permission from parents or carers is obtained before photographs of pupils are published on the school Web site
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children
- Pupils' full names will not be used on the school web site, particularly in association with photographs
- ***Parents are clearly informed of the school policy on image taking and publishing***

Social networking and personal publishing on the school learning platform

- The use of social networking sites in school is not allowed
- Pupils and parents will be strongly advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils through parent E-safety communications
- Pupils will be advised never to give out personal details of any kind which may identify them or their location

Managing filtering

- The school works in partnership with Surrey County Council to ensure systems to protect pupils are reviewed and improved

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-safety Coordinator
- Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

Managing videoconferencing

- Video conferencing/Skype will use the educational broadband network to ensure quality of service and security rather than the Internet
- Video conferencing/Skype will only take place through appropriate teacher supervision

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 or Tablets and associated cameras will not be used during lessons or formal school time, except in specific circumstances where they are specifically required
- Staff will use a school phone where contact with pupils is required

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 'Acceptable User Policy' ' 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
- Teaching staff demonstrate effective use of the internet and access to the Internet is by direct adult supervision using approved on-line materials
- Parents will be asked to sign and return an internet 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 nature of the internet, 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 audits ICT use and emergence of new technologies 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 are shared with pupils
- E-safety rules are posted in all school learning areas where the internet is accessed
- Pupils are informed that network and Internet use will be monitored
- The school uses the Surrey E-safety scheme of work and iCompute modules in order to teach children about relevant E-safety issues and instil a set of safe behaviours when accessing the internet
- E-safety lessons are taught regularly and progressively throughout the school with links to the PSHE policy

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
- 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 the school brochure and on the school web site
- On an annual basis the school will hold E-safety information sessions for parents and carers to attend
- The school will maintain a list of recommended E-safety resources for parents/carers to use in reinforcing messages of online safety outside of school
- The school will ask all new parents to sign the parent/pupil acceptable user agreement when they register their child with the school

Autumn 2014