Online Safety Policy

Review date: October 2017

Next review: October 2018

The school's Online Safety coordinator is Mrs L Athersuch

Mrs Goodfellow and Mrs Athersuch are fully trained e-safety officers

This policy should be read in conjunction with the following policies:

- ICT/Computing Curriculum Policy
- ICT Network & Equipment Terms of Use
- Code of Conduct for Students and Supply Teachers
- Acceptable Use Agreement
- Anti-bullying Policy
- Child Protection & Safeguarding Policy

Our Online Safety Policy has been written by the school, building on best practice and government guidance.

At Ashley CofE Primary School we recognise that Internet and digital communications are important and that Internet use can enhance learning for our children. The Internet is an essential element in 21st century life for education, business and social interaction. We have a duty to provide students with quality Internet access as part of their learning experience. In addition, Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

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
- The school Internet access is provided by Surrey RM and includes filtering appropriate to the age of pupils

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use through discreet and embedded teaching
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Keeping Pupils Safe

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law
- Pupils should be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

MANAGING INTERNET ACCESS

Information system security

- School ICT systems security will be 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 parent email communication must only take place via a school email address or @scopay.com
- 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. Staff or pupils personal information will not be published.
- 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. The school will use recognisable photos of individual children unless parents object.
- Only pupils' first names will be used on the website, as appropriate, including in blogs, forums or wikis
- Children's names will not be used in direct association with photographs on the school website
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking

- 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, through discreet teaching, whole school assemblies and in cross-curricular opportunities.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of 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 and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Coordinator and recorded.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Videoconferencing/Skyping will be done through the school's Skype account and should be supervised by an adult.
- 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 or for playing music through the aux cable provided. The sending of abusive or inappropriate text messages is forbidden.
- Games machines including the Sony Playstation, Microsoft Xbox and others 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 will adhere to the code of conduct when using mobile devices – iPads.

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.

- **At Key Stage 1, 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 and use a restricted log on.

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 Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

Handling Online 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 safeguarding nature must be dealt with in accordance with school safeguarding 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 Online Safety policy.

COMMUNICATIONS POLICY

Introducing the Online Safety policy to pupils

- Appropriate elements of the online safety policy will be shared with pupils.
- Online safety rules will be posted in all classrooms and areas where children may have access to the Internet.
- Pupils will be informed that network and Internet use will be monitored.

- Curriculum opportunities to gain awareness of online safety issues and how best to deal with them will be provided for pupils through discreet and cross-curricular opportunities and through whole school assemblies.

Staff and the Online Safety policy

- All staff have access to the online 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 online safety policy in newsletters, the school brochure and on the school website.
- Parents and carers will from time to time be provided with additional information on online safety.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.