Littleton C of E Infant School

E-Safety Policy

The e-Safety Policy relates to other policies including those for ICT, anti-bullying and child protection.

- Littleton's e-Safety Leader is Rachel Barton

- Our e-Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by teaching staff and approved by governors.

- The e-Safety Policy and its implementation will be reviewed annually

<u>Teaching and Learning</u>

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 children.

Internet use will enhance learning

- The school internet access is provided by Surrey County through the Easy Net contract and includes filtering appropriate to the age of children.

- Children will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

- 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 shown how to publish and present information appropriately to a wider audience.

Children 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 children complies with copyright law.

- Children should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Children will be taught how to report unpleasant internet content, e.g. Using the CEOP Report Abuse icon.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly

- Virus protection will be updated regularly by our ICT consultants – Turn IT On

- Security strategies will be discussed with the Local Authority

Email

- Children and staff may only use approved email accounts on the school system.

- Children must immediately tell a teacher if they receive offensive email.

- Children must not reveal personal details of themselves or others in email 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 email should be treated as suspicious and attachments not opened unless the author is known

- The school will consider how email from children to external bodies is presented and controlled

- The forwarding of chain letters is not permitted

Published content and school web site

- The contact details on the website should be the school address, email and telephone number. Staff or children personal information will not be published

- The headteacher or bursar will take overall editorial responsibility and ensure that content is accurate and appropriate

Publishing pupil’s images and work

- Photographs that include children will be selected carefully and will not enable individual children to be clearly identified. The school will look to seed to use group photographs rather than full face photos of individual children.

- Children’ full names will be avoided on the website 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 children 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 and personal publishing on the school learning platform

- The children will be discouraged from using social networking as they are not of the legal age required. We will request that parents be vigilant about their children accessing social media sites at home.

- Children will be advised never to give out personal details of any kind which may identify them or their location

- Children must not place personal photos on any social network space

- Children and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged children

- Children will be advised to use nicknames and avatars when using social networking sites through Lucy Faithfull Foundation Training

Managing filtering

- The school will work in partnership with Surrey County Council to ensure systems to protect children are reviewed and improved

- If staff or children come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator

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

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 allowed in school. All children with mobile phones must have them signed in and out of the school office at the start and end of the school day. The sending of abusive or inappropriate text messages is forbidden.

- Staff will use a school phone where contact with children is required.

- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

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

- At Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.

- 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 the ICT subject leader.

- 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

- Children and parents will be informed of the complaints procedure

- Children and parents will be informed of consequences for children misusing the Internet

- Sanctions within the school discipline policy include:

- Sanctioning the child with the existing behaviour policy
- Informing parents and carers
- Removal of internet access for a period

Community use of the internet

- All use of 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 children

- Appropriate elements of the e-Safety Policy will be shared with children.

- E-safety rules will be clearly visible near the school computers.

- Children 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 children.

Staff and the e-Safety Policy

- All staff will be given the School e-Safety Policy and its importance explained.

- All staff will receive e-safety training updates annually

- 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 newsletters, the school brochure and on the school web site and learning platform.

- Parents and carers will from time to time be provided with additional information on e-safety.

Date approved by the Staff and Governing Body: September 2017
Date to be reviewed: September 2018