CHRIST CHURCH INFANT SCHOOL

E-SAFETY POLICY

Date last Reviewed: Autumn 2017
Date to Review: Autumn 2018

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

- The school designated E-safety coordinator is Stella Coles
- The E-safety Policy and its implementation will be reviewed annually
- The E-safety Policy was revised by Stella Coles

What is e-safety?
E-safety encompasses internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing.

E-safety highlights the need to educate children about the benefits and risks of using internet technologies and electronic communications and provides safeguards and awareness for users to enable them to control their online experience.

Teaching and learning

Why Internet and digital communications are important

Technology is an integral part of society which children will encounter in every aspect of their lives.

The school Internet access will be designed specifically for pupils use and includes filtering appropriate to the age of children. During class ICT lessons, the children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. The internet will be deployed and integrated into all planning to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of children.

Staff should guide children in online activities that will support the learning outcomes planned for the children's age and maturity and educate them in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

If staff or children discover unsuitable sites, the URL (address), time, date and content must be reported to the ICT and e-safety coordinator and the Head of School. This information will be passed on to the LEA e-safety officer.

Schools should ensure that the use of internet-derived materials by staff and by children complies with copyright law.

Children should be taught at a time appropriate to them to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

How use of the internet is kept safe

The school Internet access will be designed specifically for pupils' use 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. The deployment of the internet will be used and integrated into planning to enrich and extend learning activities.

Access levels will be reviewed to reflect the curriculum requirements and age of children. The use of LearnPads ensures that children are directed and kept on selected websites.

Staff should guide children in on-line activities that will support the learning outcomes planned for the children's age and maturity and educate them in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Managing Internet Access

Information system security

- School ICT systems security is reviewed regularly
- Virus protection is installed and updated regularly
- Security strategies are discussed with the Local Authority

E-mail

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

Published content and the school website
- The contact details on the school website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published
- The Head of School has overall editorial responsibility and ensures that content is accurate and appropriate

Publishing pupils' images and work

Written permission from parents or carers is obtained before photographs of pupils are published on the school website or learning platform.

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

Pupils' full names will not be used on the school website or learning platform, particularly in association with photographs.

Parents are clearly informed of the school policy on image taking and publishing.

Social networking and personal publishing

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

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
- Staff will use a school phone where contact with parents or 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 Use 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 will demonstrate effective use of the internet and access to the internet is by direct adult supervision using approved online 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 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 of School
- 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

- 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 in order to teach children about relevant E-safety issues and instil a set of safe behaviours when accessing the internet. E-safety is taught throughout the school and 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 in place clear procedures for reporting issues
- Staff should not use personal email or mobile technology to contact students; if contact is necessary school telephone / email account should be used
- In the course of safeguarding updates, staff will be informed of any emerging information about E-safety

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 agreement when they register their child with the school