Colman Infant School

Policy: E-Safety Policy
Agreed by Staff: January 2015
Agreed by Governors: February 2015
Reviewed: annually
Author: Carrie Barber

Colman Infant School holds the UNICEF Rights Respecting Schools Award. Opportunities to teach children about the United Nations Charter for the Rights of the Child are sought wherever possible.

This policy is intended to set out the school's E-Safety procedures. It aims to keep children safe and protect them from potential harm. It sets out the expected behaviour and our responsibility. We recognise that the internet is an essential element in modern day life for education, business and social interaction and therefore we need to teach children to be safe and responsible users who make judgements about what they see, find and use.

Access to computers should enhance learning through:

- Enriching the quality of curriculum provision and extending learning activities
- Helping raise pupil's attainment
- Supporting teachers' planning and resourcing of lessons
- Enhancing staff development through access to educational materials, as well as the sharing of information and good curriculum practice between schools, the LEA, etc.

Agreed Procedure

- **Teaching E-Safety**
  - Pupils are taught to use technology purposefully, safely and respectfully, keeping personal information private.
  - Pupils are taught to tell an adult if they have concerns about content or contact on the internet.
  - Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
  - E-safety should be taught through Computing lessons, class teaching and assemblies.

- **Filtering:**
  - The school will use the filtering system provided by the Local Education Authority, to filter and protect users from accessing inappropriate material.
  - If staff or pupils discover unsuitable sites, the URL must be reported to the E-Safety Co-ordinators, who will report it to ICT Shared Services.
  - Any material that the school believes is illegal must be reported to the E-Safety Co-ordinators, who will report it to both CEOP and ICT Shared Services.

- **Internet Access:**
  - The Acceptable Use agreement should be signed prior to pupils and staff using the internet in school. It must also be signed by all governors, parents, volunteers and visitors who use the internet in school. All use of the school internet connection should be in accordance with this.
  - The school internet should only be used for work purposes (unless permission to use the internet for private purposes has been given by the Headteacher or E-safety coordinators).
  - Pupils will only access the internet with permission from a member of staff and all internet use by pupils will be supervised.

- **Published Content:**
  - The contact details on the school website/VLE should be the school address, email and telephone number. Staff or pupils' personal contact information should not be published.

- **Use of Images:**
  - Refer to Use of Images policy.

- **Social Networking:**
  - Social networking sites are blocked by our filtering system.
  - Staff, students, governors & volunteers are not to use social networking sites to discuss school matters.

- Staff should ensure that personal use of social networking sites (Facebook, Twitter, etc) has appropriate security settings configured so that only your friends can view your profile, and that care is taken in what staff post.
- Staff should not at any time forge 'friendships' on these sites (or any similar sites) between themselves and parents of current pupils.

- **Email:**
  - Pupils and staff may only use approved e-mail accounts (nsix accounts) on the school system and to send work related emails.
  - Care should be taken to ensure that all emails have been addressed to the correct recipient(s).
  - If an e-mail concerns an individual then do not name them in the 'subject field'.
  - Pupils will be taught to use email safely during skills sessions prior to any activity and all emailing is supervised.
  - Pupils must immediately tell a teacher if they receive an offensive e-mail or report it using the whistle blowing button on the VLE.
  - 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 Virtual Learning Environment and will be monitored.
  - Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
  - Users must not forward on chain letters or joke emails.

Is this working?

- Is there evidence, through assessment in Computing, that pupils are using technology safely and respectfully; that they are keeping personal information private; that they can identify where to go for help and support when they have concerns about content or contact on the internet?
- Is E-Safety being monitored regularly by the E-Safety coordinators?

Practical Information

- The E-Safety Co-ordinators are Carrie Barber and Janice Norman. Matthew Gamble has overall responsibility for E-Safety and therefore any complaints about internet misuse must be referred to him.
- Illegal material should be reported to:
  - CEOP (Child Exploitation and Online Protection): http://www.ceop.police.uk/