St Cuthbert's RC Primary School

E-Safety Policy

At St Cuthbert's RC Primary School, E-safety is a core responsibility. The need to protect children from significant external risk on the internet, and the need for direct teaching of responsible and safe IT practices are a vital part of modern day education.

The E-Safety Policy directly relates to other policies including those for Computing and Safeguarding. Our school policy has been developed from the Kent E-Safety Policy and government guidance.

Teaching and Learning:

Rationale:

The internet is an essential part of education, business and social interaction in the 21st century. Pupils need to learn how to evaluate Internet information and to take care of their own safety and security. The school has a duty to provide pupils with quality Internet access as part of their learning. Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

The purpose of Internet use in school is to raise educational standards, promote pupil achievement, support the professional work of staff and to enhance the school's management functions.

Use of the Internet to Enhance Learning:

The school's Internet access is designed to enhance and extend education:

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils and provided by DurhamNet, the County approved provider.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils, with their parents, have to sign an agreed 'Rules for Responsible Use of IT' contract when starting school. The rules are prominently displayed around school.
- 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 to a wider audience.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Evaluating Internet Content:

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. As pupils mature, they will be taught the importance of cross-checking information before accepting its accuracy.

- Pupils will be taught to report unpleasant Internet content (including images, text etc that make them feel uncomfortable) to the member of staff in charge of that group of children. This information will be logged by the E-safety coordinator and dealt with appropriately.

Managing Internet Access:

- School IT systems security will be reviewed regularly
- Virus protection will be updated regularly by the school technician
- Security strategies will be used as advised by the Local Authority, linking to DurhamNet Filtering and actual access to the school network.

E-mail:

- Pupils may only use approved e-mail accounts on the school system. These are Durham LA accounts.
- Pupils must tell a teacher immediately if they receive offensive e-mail.
- Pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission via e-mail communication.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. This applies to both staff and pupils.
- The forwarding of chain letters is not permitted.

Published Content and the School Website:

- Personal contact information, for staff or pupils, will not be published on the school website.
- The Head teacher will take overall responsibility to ensure that content is accurate and appropriate

Storing and Publishing Pupil Information, Images and Work:

- All teaching staff have an encrypted memory stick. This will be used in the event that staff need to store a pupils information (shot-term only) for use outside of school.
- Photographs that include pupils will be carefully selected so that individual pupils cannot be identified or their image misused. We will always aim to use group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on our school website or other online space.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

- Pupil image file names will not refer to the pupil by name.
- Photographs of pupils should be stored on the secure DLG platform, not on staff computers or memory sticks.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social Networking and Personal Publishing:

- The school will deny access to known social networking sites, and consider how to educate pupils in their safe use. Pupils will be educated regarding the risks linked to social network sites, in order to develop safe and responsible online behaviours.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils will only use moderate social networking, such as Durham Learning Gateway.
- Parents will be given signposts to websites where they can gain information on supporting and reinforcing the E-safety messages promoted within school.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing Filtering:

The school will work with Durham LA to ensure systems to protect pupils are reviewed and improved.

If staff or pupils come across unsuitable online materials, the site must be reported to the E-safety Coordinator.

Managing Video Conferencing and Webcam Use:

Video conferencing should use the educational broadband network to ensure quality of service and security. Pupils must ask permission from the supervising teacher before making or answering a video conference call. Video conferencing and webcam use will be appropriately supervised.

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.

The IT coordinator and the Leadership Team should note that technologies such as mobile phones with wireless Internet access can bypass the school filtering system and present a new route to undesirable material and communications.

- Pupils are not allowed to bring mobile phones to school without the prior consent of the Head Teacher. The phone must then be handed to a member of staff and kept in the Office until the end of the day.

- The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden
- The use of cameras in mobile phones is forbidden.
- If staff need to use their mobile phones to contact parents/pupils (eg on school trips) they should withhold their number to prevent parents/pupils gaining access to staff personal phone numbers.

Managing a Learning Platform (PL):

An effective learning platform can offer schools a wide range of benefits to teachers, pupils and parents, as well as support management and administration.

Safeguarding Lead: Mrs C. Swales

E- Safety Lead: Mrs H. Bewley