Cardinal Newman Catholic Primary School

E-safety policy

Writing and reviewing the E-safety policy

The E-safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

- **The school will appoint an E-safety coordinator. This will be the ICT Coordiantor.**
- Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors
- The E-safety Policy and its implementation will be reviewed annually
- The E-safety Policy was revised by: ……………………………………………
- It was approved by the Governors on: ……………………………………….

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
- Staff and pupils will access the internet when using the school's learning platform
- The school Internet access is provided by Surrey County through the EasyNet contract 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
- 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.

Pupils 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 pupils complies with copyright law
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- 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 do not have individual e-mail accounts: each class has a class e-mail account accessible to all children which is password-protected and may only be used under teacher supervision.**
- 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 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 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 and will not enable individual pupils to be clearly identified. The school will look to seek to use group photographs rather than full-face photos of individual children
- Pupils' full names will be avoided on the Web site 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 pupils are published on the school Web site
- 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 school will not allow access to social networking sites.
- Specific newsgroups will be given access only.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils

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 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 videoconferencing

- In the future, videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- 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. The sending of abusive or inappropriate text messages is forbidden
- Staff will use a school phone where contact with pupils 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

- All staff must read and sign the 'E-Safety Policy for Staff, Governors and visitors' 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.

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 a senior member of staff
- Any complaint about staff misuse must be referred to the head teacher

- 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

- Appropriate elements of the E-safety policy will be shared with pupils
- E-safety rules will be posted in all networked rooms.
- Pupils 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 pupils

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 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
- Parents and carers will from time to time be provided with additional information on E-safety
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.