St Mary's Catholic Primary School

E-Safety Policy

Person Responsible: Miss C. Dineen

Date: September 2016

Review date: Autumn 2017

Approved by Governors:

The school's e-Safety Officer is <u>Miss M Jackson (Headteacher)</u>

The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for ICT, bullying, child protection and photographic images of children. It builds upon the London Grid for Learning (LGfL) exemplar policy.
We recognise it is our duty as educators to ensure every child is safe and this policy is drawn up to provide guidance on how to minimise risks and deal with any infringements.

Teaching and learning

Why Internet use is 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.

Internet use will enhance learning
- The school Internet access will be designed expressly for pupil use and will include 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 taught how to evaluate Internet content
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will know how to alert the appropriate people if they come across something they do not like.
- Pupils will be aware of how to manage their own internet use when not on site.

Managing Internet Access

Information system security
- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Greenwich and will be in line with LGfl guidance.
- Usernames and passwords will be used where appropriate.

E-mail
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Published content and the school web site
- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work (See Photographic images of children policy)
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Parents or carers will indicate when photographs of pupils are not to be published on the school Web site. (see e-safety rules consent form)
- Work can only be published with the permission of the pupil and parents/carers. (See e-safety rules consent form)

Social networking and personal publishing
- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised during annual e-safety training that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Managing filtering
- The school will work with Greenwich, ASK and Becta to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.

- Guidelines for safe internet use displayed in all areas with computers including steps to take to report anything which appears which children do not like.

- **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 senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

- Pupils are not allowed mobile phones except in special circumstances when permission has been granted and they are left in the school office.

- No child is to bring in tablets from home for use in 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 'Staff information systems code of conduct'

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

- All children will sign 'SAFE' acceptable use agreements to show awareness of their responsibility.

- Parents will be asked to sign and return an e-safety rules consent form.

Assessing risks
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Greenwich can accept liability for any material accessed, or any consequences of Internet access.

- Through E-Safety sessions teachers will attempt to monitor any age inappropriate use of the internet/ social networking sites. Any concerns will be passed to the E-Safety officer and parents.

- 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.

- Children will not be unsupervised when using technology with access to the internet.

- AB Tutor allows teachers to monitor student activities within the ICT suite.

Handling e-safety complaints

- Discussions with children/ staff member involved.
- Keep a record e.g. print out, of any inappropriate content.
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- 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.
- Pupils and parents will be informed of the complaints procedure. (see school complaints policy)

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils regularly.
- Pupils will sign SAFE code of conduct.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-safety is embedded within the ICT scheme of work and is based on the materials from CEOP.

Staff and the e-Safety policy

- All staff will know how to access 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 work to clear procedures for reporting issues.
- Staff will receive E-Safety training to ensure an up to date knowledge.
- Staff will strive to use a child friendly safe search engine when accessing the web with pupils.
- Governors have an overview of the E-Safety policy, issues and strategies within the school, and are invited to attend E-Safety training within school.

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.
- The school will maintain a list of e-safety resources for parents/carers.
- Parents will be encouraged to attend annual e-safety training.
- Parents are asked to sign e-safety rules consent form.