St. Mary's Catholic Primary School

E-Safety Policy

March 2024

Next review date: March 2026

The E-safety Policy should be read in conjunction with policies including those for ICT, Data Protection, Anti-bullying, Safeguarding and for Child Protection. It 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 Head teacher will be responsible for the overview of E-Safety, supported by the computing coordinator.

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 curriculum and a necessary tool for staff and pupils and the school Internet access is provided by Securly and includes filtering appropriate to the age of pupils.

At St. Mary's Catholic Primary School:

• 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

• 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 will 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.

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 IT provider - Magika

E-mail

• Pupils may only use approved e-mail accounts on the school system, and staff may only use accounts from filtered providers.

• Pupils will be taught not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission, and of the dangers associated with such behaviour.

• Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Published content and the school web site

• The contact details on the Website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.

• The Headteacher and the IT coordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing photographs, images and work

• Written permission from parents/carers will be obtained for the taking and publishing of photographs or video.

• Photographs that include pupils will be selected carefully and 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.

• 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 on the school learning platform

• Pupils will not have access to social networking sites at school, but the school will educate pupils in their safe use e.g. use of passwords.

• They will be advised never to give out personal details of any kind which may identify them, anybody else or their location.

• Pupils, parents and staff will be advised on the safe use of social network spaces

• Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

• If staff or pupils come across unsuitable on-line materials, the site must be reported to the nominated member of staff.

• The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- Securly informs the Headteacher if there have been blocked searches made by pupils.

Managing videoconferencing

• Any videoconferencing will take place in the structured context of lessons at this school.

• 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.

Other devices

• Mobile phones and associated cameras will not be used in school by pupils or staff

• The sending of abusive, offensive or inappropriate material is forbidden (See Anti-bullying policy).

• Staff should not share personal telephone numbers with pupils and parents, unless they are personal friends. (A school phone will be provided for staff where contact with 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

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

• Parents will be asked to sign and return a consent form.

• Pupils must agree to comply with the Responsible Internet Use statement before being granted Internet access.

• Any person not directly employed by the school will be asked to sign an 'acceptable use of school IT resources' form before being allowed to access the Internet on 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.

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 referred to the Designated Safety Lead for Safeguarding and 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 and pupils will sign an acceptable use policy annually.

Enlisting parents' support

• Parents' and carers attention will be drawn to the School E-safety Policy in newsletters 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.