

Holy Family
Catholic Primary School



E-Safety Policy

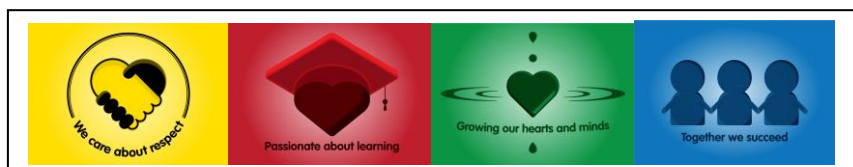
Approved March 2021

Review date March 2024



E-SAFETY POLICY **(see also Computing Policy)** **Mission Statement and School Values**

At Holy Family we grow, learn and succeed in the footsteps of Jesus.



Teaching and Learning

The Internet is an essential element in life for education, business and social interaction. Holy Family Catholic School has a duty to provide pupils 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 will enhance learning.

The school Internet access will be designed expressly for pupils 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.

The new National Curriculum states that pupils should be taught to:

	<u>Key Stage 1</u>	<u>Key Stage 2</u>
<u>Digital Literacy</u>	Recognise common uses of information technology beyond school Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies	Understand the opportunities [networks] offer for communication and collaboration. Be discerning in evaluating digital content Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact

Authorised Internet Access

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

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- All children will sign an 'acceptable use agreement' when they have discussed all the points mentioned in the policy.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the e-safety coordinator or network manager.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- 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.
- Whole class or group e-mail addresses should be used in school
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking

- Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with the Local Authority, and the Internet Service Provider to ensure filtering systems are as effective as possible.

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 will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

Published Content and the School Website

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Work and photographs

- Pupil and parental consent should be sought prior to publication.
- Pupils' full names and other personal information should be omitted.
- Pupils should be supervised. Only sites that are secure
- Work can only be published with the permission of the pupil and parents.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

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. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

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 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.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Introducing the e-safety Policy to pupils

E-Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. Pupils will be informed that network and Internet will be monitored.

Staff and E-Safety Policy

All staff will be given the School e-safety Policy and its importance explained. Any information downloaded must be respectful of copyright, property rights and privacy. Staff should be aware that Internet traffic can be monitored and traced to individual user. Discretion and professional conduct is essential. A laptop issues to a member of staff remains in the property of the school. Users of such equipment should therefore adhere to

school policy regarding appropriate use with regard to Internet access, data protection and use of software.

Enlisting parent's support

Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school website. An annual e-Safety meeting will be held for parents.

Using Search engines

Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.

- Web quests e.g. Ask Jeeves for kids
- Kidzsearch
- CBBC search

Exchanging information with other pupils

Pupils should only use approved email accounts- '2email'
Pupils should never give out personal information

User agreement- Appendix A

Permission for photographs- Appendix B