# E-SAFETY POLICY


## HOLY FAMILY CATHOLIC PRIMARY SCHOOL

Written and agreed: November 2020
Review date: November 2021

Holy Family Catholic Primary School pledges itself to be a place where uniqueness is celebrated and all individuals will find safety and respect for themselves, their families and their way of life.

Electronic technologies are an essential part of 21st century life. This E-Safety Policy reflects the need to raise awareness of the safety issues associated with electronic communications as a whole. This policy will be displayed on the school website and should operate in conjunction with other school policies including;

- Safeguarding Policy
- Positive Behaviour Management Policy
- Social Media Policy
- Computing and ICT Policy
- Staff Code of Conduct

The E-Safety Policy will be reviewed annually by the SLT using relevant guidance and has been formulated using guidance from LCC Acceptable Use Code of Practice.

## 1) Teaching and Learning

### 1.1 Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-safety is therefore an essential part of the school's E-safety provision. Children and young people need the help and support of the school to recognise and avoid E-safety risks and build their resilience. **See appendix 1 – Appropriate Internet Use**

E-safety should be a focus in all areas of the curriculum and staff should reinforce E-safety messages across each subject. The Computing curriculum includes an E-safety topic for each year group, which needs to be continually reinforced. These topics will adhere to the principles of the relevant E-Safety sections of the DFE

**2014 National Curriculum Programmes of Study for Computing:**

KS1

- 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.

KS2

- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

We continually strive to ensure:

- 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.
- That the use of Internet derived materials by staff and pupils comply with copyright law.
- Pupils understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are 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 deal with inappropriate information online or what to do when they feel threatened or uncomfortable.
- Pupils will be taught not to reveal personal details of themselves or others in email or online communication, or arrange to meet anyone without specific permission.

### 1.2 Parents and Carers

Many parents and carers have only a limited understanding of E-safety risks and issues, yet play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimated how often children and young people come across potentially harmful and inappropriate material on the internet and through gaming and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through;

- Specific online safety page on the school website

- Newsletters and letters
- Published Magazines
- Events and campaigns (Eg; Safer Internet Day)
- Parents training and courses

## 2) Managing Internet Access

### 2.1 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 other providers.

### 2.2 School website www.holy-family.co.uk

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 head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Pupils' full names will not be used anywhere on the website, particularly in association with photographs, which will be selected carefully. Written permission from parents or carers will be obtained for photographs of pupils to be published on the school website and other social media.

### 2.3 Social networking and personal publishing

The school will block/filter access to social networking sites (excluding Twitter – see Social Media Policy). 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 is inappropriate for primary aged pupils without guidance or education. Any issues on Social Media which impacts on school life will be dealt with in by a member of Senior Leadership Team. The use of such systems by teaching staff should be compatible only with their professional role. **(User Code of Conduct for ICT – Appendix 2).**

### 2.4 Managing filtering

The school will work with the LA, DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. Smoothwall web filtering issues are emailed to HT email address for monitoring purposes. Some sites (such as Twitter and You Tube) will be unlocked for educational purposes but must be used appropriately and monitored by staff members **(Appropriate Internet use – Appendix 1).** If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Lead. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

COVID-19: Laptops on loan during isolation periods will be managed through the Meraki monitoring system to ensure safe use when children are accessing online learning.

### 2.5 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 during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. Staff must use a school phone where contact with pupils is required.

### 2.6 Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

## 3) Policy Decisions

### 3.1 Authorising Internet Access

All staff must read and sign the **'Acceptable Use Policy' (See Appendix 2)** before using any school ICT resource. At key stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. In the Computing Curriculum units of work will be dedicated to staying safe online.

### 3.2 Assessing Risks

The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT provision on an ongoing basis to establish if the e-safety policy is adequate and that its implementation is effective. However, children will also be taught about e-safety risks, how to minimise these and dealing with them if they arise.

### 3.3 Handling E-Safety Complaints

Pupil Internet misuse will be dealt with by a senior member of staff and will be dealt with in accordance with the Behaviour Policy. Staff will be aware of expectations placed upon them through the Code of Conduct and **'Users Code of Conduct for ICT (see appendix 2).** 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 safeguarding procedures.

## 4) Unsuitable/inappropriate activities

School ICT systems are only to be used for agreed, appropriate and suitable work related activities. Internet activity which is considered unsuitable or inappropriate will not be allowed and if discovered will lead to disciplinary action. Internet activity which is illegal will be reported and could lead to criminal prosecution.

Computing Lead: Laura Lacey

Date of Policy: November 2020

Review date: September 2021