# St. Joseph's Catholic Primary School

# E-Safety Policy

St. Joseph's Catholic Primary School takes seriously the safety of all its pupils. In particular, this relates to learning that may take place through the use of electronic devices. The following document was drawn up in consultation with staff, Governors, pupils and parents/carers to further safeguard its pupils.

Our e-safety policy should be read in conjunction with other pupil safeguarding policies including those for Computing, Anti-Bullying, Child Protection and Data Protection.

Our school has a named E-safety Co-ordinator, Miss Trudie David.

Our E-Safety Governor meets annually with the E-Safety Co-ordinator.

Our e safety policy has been written building on the LBBD E-safety Policy and government guidance. It has been agreed by senior management and approved by governors.

**Teaching and Learning**

**Why the Internet and Digital Communications are Important:**

The Internet is an essential element in 21st century life for education, business and social interaction. We understand that as schools we have 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 our staff and pupils.

**Internet use will enhance learning:**

The schools' internet access has been designed expressly for pupil use and includes filtering appropriate to the age of pupils. Filtering is implemented through the London Borough of Barking and Dagenham ISP.

Pupils are taught about acceptable and unacceptable internet use and practice. Our children are provided with clear objectives for internet use.

Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

**Pupils are Taught How to Evaluate Internet Content:**

We seek to ensure that the use of internet derived materials by staff and pupils complies with copyright law.

Pupils are taught the importance of cross-checking information before accepting its accuracy.

Pupils are taught how to report inappropriate internet content.

**Managing Information and Communication Systems**

**Information System Security:**

The school computing systems are reviewed annually by the Governing Body.

We regularly check that the virus protection is updated and inform the Local Authority of any issues.

Security strategies are always discussed with the Local Authority.

**Password Policy:**

Strong passwords for adult users on the staff network are essential.

As per the staff AUP, users agree not to logon using any other username/password.

**Data Transfer Off Site:**

Only permanent members of teaching staff who have read and signed the AUP may transfer pupil data off site.

Highly sensitive data such as a full SIMS list including surname and home addresses, detailed medical, educational and personal information may only be transported on an encrypted memory stick and then only with permission from the Headteacher.

When one or more teachers are contributing to end of year reports it is important that the documents are only transported via school approved encrypted memory stick, or school email using the secure system.

Encrypted memory sticks for school use are an individual user's responsibility and should not be shared. For the purpose of collaboration, users should transfer relevant files to a secure shared location such as the school network or a school network workstation.

Staff working with school data off site have a duty to prevent non-school staff viewing screens, as per the AUP.

All staff must check any files they propose to use in school are free from virus/spyware/ malware. Staff understand that it is their responsibility to ensure that any material contained files they put on the school network are fit for the purpose of teaching and learning.

**Email:**

Pupils may only use e-mail accounts on the school system which are approved by the school. Pupils must immediately tell an appropriate member of staff if they receive any offensive e-mail.

Staff should only use their school email account in communication with pupils, parents and other staff in a professional manner.

In email communication, pupils are trained not to reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Pupils are educated (in appropriate year groups), in how to deal with incoming email and associated attachments.

Currently only internal emails are exchanged. Should we communicate through emails with other users we will consider how email from pupils to external bodies is presented and controlled.

**Published Content (Printed or Online):**

Staff or pupil personal contact information is not published. In general contact details given online is served through the school office. Where pupils link with other schools their individual mail address is used. These mails are monitored.

The Headteacher has overall accountability and ensures that published content is accurate and appropriate.

**Publishing Pupils' Images and Work:**

All parents/guardians must sign the digital media release form to give their consent before photographs are used.

Digital media is used in accordance with the home school agreement.

The digital media release form is reviewed annually.

**Social Networking and Personal Publishing:**

Currently our school does not engage in social networking sites. Should this policy change:

- We will control access to social networking sites, and where relevant educate pupils in their safe use.
- All newsgroups, forums and chat-rooms will be blocked unless a specific use is identified.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils would use only monitored social networking sites.

Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Pupils will be advised to use nicknames and avatars (icons / characters used to represent user) when using social networking sites.

**Managing filtering:**

The Hard Federation of St. Joseph's Primary Schools works with the Local Authority to ensure systems to protect pupils are reviewed and improved.

If staff or pupils come across unsuitable on-line materials, the site is reported to the computing subject leader immediately in line with school policy.

Senior staff and the computing subject leader ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

**Managing video-conferencing and webcam use:**

Video-conferencing uses the educational broadband network to ensure quality of service and security rather than the Internet.

Pupils must ask permission from the supervising teacher before making or answering a video-conference call.

Video-conferencing and webcam use is appropriately supervised for the pupils' age.

**Managing emerging technologies:**

Emerging technologies are examined for educational benefit and any risks considered before use in school is allowed.

The senior leadership team have noted 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.

The use of mobile technologies during school time is not permitted. The sending of abusive or inappropriate data is forbidden.

The use by pupils of cameras in mobile phones is not permitted.

Games machines including the Sony Playstation, Microsoft Xbox and others that have Internet access which may not include filtering, should these be used, the Federation will closely monitor their use in the schools or in any other officially sanctioned location.

Staff have access to a school phone if contact with pupils is required.

**Protecting personal data**

Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998 and any other relevant legislation.

**Policy Decisions**

**Authorising Internet access:**

All staff have read and signed the Staff Acceptable Use policy before using any school IT resource.

Parents / carers have signed a consent form giving their permission for their child to use the Internet in school. Our pupils have signed an e-safety agreement form indicating they are aware of the rules of conduct when using the Internet and other IT resources.

Our school has a current record of all staff and pupils who are granted access to school IT systems.

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

**Assessing risks:**

St. Joseph's Catholic School takes 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 LBBD can accept liability for any material accessed, or any consequences of Internet access.

The school audits IT use to ensure that the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

**Handling e-safety complaints:**

Any complaints of internet misuse are dealt with initially by the E-safety Co-ordinator and by a senior member of staff where necessary and as appropriate.

Any complaint about staff misuse is referred to the Head Teacher.

Any complaints of a child protection nature are dealt with in accordance with Safeguarding/Child Protection procedures.

Pupils and parents are informed of the complaints procedure (see school complaints policy).

Pupils and parents are informed of consequences for pupils misusing the Internet.

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

**Community use of the Internet:**

The school liaises with local organisations to establish a common approach to e-safety.

**Communications Policy**

**Introducing the E-safety Policy to Pupils:**

E-safety rules are posted in all rooms where pupils may use IT equipment and are discussed with pupils at least termly.

Pupils are informed that network and Internet use is monitored and appropriately followed up.

A programme of training in e-safety has been developed.

E-Safety training is embedded within the Computing scheme of work and the Personal, Social, Health and Citizenship Education (PSHCE) curriculum.

**Staff and the E-safety policy:**

All staff are given the school E-safety Policy. The policy and its importance is explained.

Staff are informed that network and Internet traffic is monitored and traced to the individual user.

Staff that manage filtering systems or monitor IT equipment use are supervised by Senior Management and work to clear procedures for reporting issues.

Staff always use a child friendly safe search engine when accessing the web with pupils.

**Enlisting Parents' and Carers' support:**

Parents' and carers' attention has been drawn to the school E-safety Policy.

St. Joseph's Catholic School asks all new parents to sign the parent/pupil agreement when they register their child with the school.

As a school we will endeavour to signpost parents/carers to suitable e-safety resources and advice.

Last reviewed: October 2024

Next review: October 2027