St Joseph's RC Primary School

E Safety Policy

St Joseph's RC Primary School

E-Safety Policy

At St. Joseph's RC Primary School we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, whiteboards, digital video equipment, etc); and technologies owned by staff, but brought onto school premises (such as laptops, mobile phones and camera phones).

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in our school is Irene Tomkins who has been designated this role as ICT Coordinator. All members of the school community have been made aware of who holds this post.

The e-Safety co-ordinator:

- Takes day-to-day-responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policy / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- Provides training and advice for staff
- Liaises with school ICT technical staff (Digitech).
- Receives reports of e-Safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with e-Safety Governor to discuss current issues, review incident logs.
- Keep abreast of current issues and guidance.

Senior Management and Governors are updated by the Head/ e-Safety coordinator.
This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community.

Managing the school e-Safety messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.

- The e-Safety policy will be introduced to the pupils at the start of each school year.
- E-Safety rules are displayed next to computers and in each classroom.

E-safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis.

- The school provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating Key Stage 2 pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member.
- Pupils are taught to critical evaluate materials and learn good searching skills through cross curricular teacher models and discussions.

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school internet access is designed for pupil use and includes filtering.
- Pupils are taught what internet use is acceptable and what is not.
- Internet access will be planned to enrich and extend learning activities.
- Staff will preview any recommended sites before use.
- Staff will guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation.
- As part of the new ICT (computing) curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line.

Authorised Internet Access

- All staff must read and sign the 'Acceptable Use Agreement' before using any school ICT resource.
- Parents are asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and internet access can be used within the school.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Headteacher or e-Safety co-ordinator. The incident will be recorded in the e-Safety Log. The e-Safety Log will be reviewed termly by the e-Safety Co-ordinator.
- 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.
- It is the responsibility of the school, by delegation to the network manager (Digitech) to ensure that Anti-virus protection is installed and kept up to date on all school machines.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. We recognise that pupils need to understand how to style an email and appropriate usage is an important part of e-safety. As part of the new curriculum pupils must have experience sending and receiving emails.

- The school gives all staff their own email account to use for all school business.
- It is the responsibility of each account holder to keep the password secure.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Access in school to external personal email accounts is not allowed.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.
-

Social Networking

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered
- 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.
- Staff will abide by the recommendations and requirements set out in the Social Networking Policy when using online social networks outside of school.

Safeguarding pupils who are vulnerable to extremism and radicalisation

St Joseph's RC Primary School is committed to actively promoting the fundamental British values of democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs; the pupils are encouraged to develop and demonstrate skills and attitudes that will allow them to participate fully in and contribute positively to life in modern Britain.

There is a current threat from terrorism in the UK and this can include the exploitation of vulnerable young people, aiming to involve them in terrorism or to be active in supporting terrorism. Staff in school seek to protect children and young people against the messages of all violent extremism including but not restricted to those linked to Islam ideology, Far Right/Neo Nazi/White Supremacist ideology etc. Concerns should be referred to the Designated Safeguarding Lead who has local contact details for Prevent and Channel referrals. They will also consider whether circumstances require the police to be contacted.

Mobile technologies

- Pupils by permission of the Headteacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office at 8:55am and collected at the end of the day.
- The school allows staff to bring in personal mobile phones and devices for their own use. **Staff must not take or store photos of students' on their Mobile phones.**
- Staff are not permitted to use mobile phones / texts during lesson time.
- Staff should always use school phone to contact parents
- Staff may use their mobile phones in the staffroom during the lunch period.
- Parents cannot use mobile phones on school trips to take pictures of the children.
- The sending of inappropriate text messages between any member of the school community is not allowed.

Safe Use of Images

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- With the written consent of parents and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others, this includes when on field trips.
- The Headteacher or nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner

Publishing pupil's images and work on the school website

- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos 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 Website, particularly in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school Web site.

E-Safety skills development for staff

- Our staff receive regular information and training on e-Safety issues in the form of staff meetings.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know to report the misuse of technology by any member of the school community to the e-Safety co-ordinator or the Headteacher.
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Pupils with Additional Needs

Staffs are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Parental Involvement

We believe that it is essential for parents/ carers to be involved with promoting e-Safety both in and outside of school.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on the school website)

Communication of Policy

Pupils

- Rules for Internet access will be posted in all classrooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe online. This will be strongly reinforced across all year groups during ICT lessons and all year groups look at different areas of safety through the digital literacy lessons

Staff

- 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.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school website.

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 network manager.
- E-safety will be discussed with our ICT support (Digitech) and those arrangements incorporated in to our agreement with them.

Protecting Personal Data

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

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 shall be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

.

Reviewing this Policy

The e-safety Policy and its implementation shall be reviewed annually