'Growing, loving and learning in the arms of Mary'

E-Safety Policy

E-Safety Policy
Review date: September 2023

What is e-Safety?

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The previous Internet Policy has been extensively revised and renamed as the Schools' E-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

Teaching and learning

Why Internet use is 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 statutory curriculum and a necessary tool for staff and pupils.
- Internet use will enhance learning.
- The school's 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.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught how to evaluate Internet content.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law as far as possible.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

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 Connected IT.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- 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.
- E-mail sent to an external organisation 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.

Managing filtering

- The school will work with the BCCET, DFe and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Leader.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The school web site

St Mary's Catholic Primary School values the contribution that a website can make to the life and role of the school in a modern society. St Mary's Catholic Primary School website has 5 important roles:

1. To promote the school
2. To provide information to prospective parents and teachers, the wider community and the world
3. To act as a communication channel between teachers, parents, pupils and school management
4. To improve pupil learning
5. To raise standards in teaching and learning.

Safeguards

The safety of children and other users who appear or are referred to on the published site and extranet is of paramount importance.

Publishing names, images and work

- Adult's names will be published as their title and last name e.g. Mr. Davies. Children's names will be published as their first name only e.g. Trevor, or if required, first name and last name initial e.g. Trevor D.
- Any images of children will not be labelled with their names.
- No close up pictures of individual children will be available online- only group photographs with two or more children (Unless parental consent has been given).
- Children will only be shown in photos where they are suitably dressed.
- Personal details of children, staff and governors, such as home addresses, telephone numbers, personal e-mail addresses, etc. will not be released via the website or school e-mail.

Privacy

- Adults have the right to refuse permission to publish their image on the published site or extranet.
- Parents have the right to refuse permission for their child's work and/or image to be published on the published site or extranet.
- Those wishing to exercise this right should express their wishes in writing to the Headteacher, clearly stating whether they object to work, images, or both being published, to the published site or internet. Parents will be notified of this right by publication of this policy on an annual basis.

Monitoring

- The class teacher will check material before it is uploaded to ensure that it is suitable and complies with the record of objections held by the Headteacher and with copyright laws (as far as is possible). Any persons named on a web page can ask for their details to be removed.
- The web pages will be regularly reviewed for accuracy and will be updated as required. This review will occur at least annually. It will be the responsibility of the Site Administrator, school management and staff to ensure this happens.

Maintenance and Editing

At least two people should have the knowledge to maintain and edit the site, and they must pass on their knowledge to a successor at the end of a term of office.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked 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 and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
-

Videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

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.
- 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

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form. Upon a non-return of the form it will be assumed that the parent has granted permission for internet use.

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 to establish if the E-Safety policy is adequate and that its implementation is effective.

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.

Communications 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 use will be monitored.

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.
- Enlisting parents' support
- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school Web site.
- Reviewing the E-Safety Policy
- The E-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.
- Our E-Safety Policy has been written by the school, building on BECTA and government guidance. It has been agreed by senior management and approved by governors.

Appendix 1

St Mary's Catholic Primary School

Pupil E-Safety Agreement

This is to be read through with your parent(s).

At St Mary's we believe that accessing the internet is of great educational benefit, however we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.

- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.
- Pupils are expected not to use any rude language in their email communications and contact only people the teacher has approved. It is forbidden to be involved in sending chain letters.
- Pupils must ask permission before accessing the Internet.
- Pupils should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet.
- No programs on discs should be brought in from home for use in School.
- Homework completed at home may be brought in on suitable media storage (eg. Flash drive, memory stick or CD/DVD-rom but this will have to be virus scanned by the class teacher before use.
- Personal printing is not allowed on our network for cost reasons (e.g. pictures of pop groups/cartoon characters).
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made.
- Pupils consistently choosing not to comply with these expectations will be warned and subsequently, may be denied access to internet resources.