St Mary's Catholic First School

E-Safety Policy

BISHOP WILKINSON

Bishop Wilkinson
Catholic Education Trust
Through Christ, in Partnership

Part of the Bishop Wilkinson Catholic Education Trust
Company Registration Number 07890590

Signed by Chair	T Neeson
Statutory Policy	Yes
Required on Website	Yes
Review Period	February 21
Next Review Date	February 22
Reviewed by	P Naughton

St Mary's Catholic First School

E-Safety Policy

The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for ICT, bullying and for child protection.

- • The headteacher will be the e-Safety Coordinator.
- • Our e-Safety Policy has been written by the school, and based on LA and government guidance. It has been agreed by staff and approved by governors.
- • The e-Safety Policy and its implementation will be reviewed annually.

Why Internet use is important

1. 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.
2. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
3. Internet use will enhance learning
4. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
5. Pupils will be taught what Internet use is acceptable and what is not, and they will be given clear objectives for Internet use.
6. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
7. Pupils will be taught how to evaluate Internet content
8. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
9. 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 regularly with the LA.

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.
- • Published content and the school web site

- The contact details on the Web site 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.
- Photographs that include pupils will be selected carefully. These will be group photographs not individual pupils photographs.
- Pupils' full names will not be used on the Web site in association with photographs.
- Pupils' work can only be published with the permission of the pupil and parent.

Social networking

- 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 should be closely monitored and treated with caution for middle school pupils.

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.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.
- The technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

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

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 be not used during lessons or normal 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 be aware of the e-safety policy before using any school ICT resource.

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

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 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 the teacher responsible for behaviour and/or the headteacher.
- 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 as set out in the child protection policy.
- Discussions will be held with the police to establish procedures for handling potentially illegal issues.

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, and on the school Web site.
- Parents should ensure that children are using the Internet safely and responsibly at home.
- Parents will be advised to visit "Know It All" website - a guide to getting the most out of the Internet and keeping children safe online.

Addendum

Online learning

During periods when pupils require access to online learning provided by St. Joseph's teachers:

•   At least two members of staff will have access to communications between staff and pupils.
•   Teaching staff will have the responsibility to monitor any communication between pupils in open class comments sections.