St Mary's Catholic Primary School

E-Safety Policy

A Community where we live, learn and laugh together in God's love.

Updated for the academic year:

2017-18

Rationale

In St Mary's Mission Statement we highlight our commitment to providing 'a secure environment in which quality of life, enjoyment of school, self esteem, a respect of others and a sense of personal and collective achievement can be found'.

We are therefore committed to safeguarding and caring appropriately for every aspect of the lives of the children in our school.

We recognise our responsibility to take action on behalf of children and others who are, or may be, at risk of physical neglect or from physical, sexual or emotional abuse at the hands of any other person.

School Responsibilities

The school will appoint an e-Safety Coordinator. This may be the Designated Child

Protection Coordinator as the roles overlap. The Head teacher is the current appointee.

Our e-safety Policy has been written by the school, building on the KCC e-safety

Policy and government guidance. It has been agreed by the senior management and approved by governors.

The e-Safety Policy and its implementation will be reviewed annually.

Teaching and learning

Purpose of Internet use in school

Internet use is part of the statutory curriculum and a necessary tool for learning.

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 and safe Internet access as part of their learning experience via specific sites or agreed search engines.

Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security

Benefits of Internet use

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;

- exchange of curriculum and administration data with DfES;
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

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.

Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How will pupils learn how to evaluate Internet content?

The Head teacher will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

Pupils will be taught to understand that when using Internet material they need to acknowledge the source.

The evaluation of on-line materials is a part of every subject.

Managing Information Systems

Security of the school information systems

The security of the school information systems will be reviewed annually by the Computing Manager.

Virus protection will be updated regularly. Security strategies will be discussed with EXA and PC Warehouse.

Personal data sent over the Internet will be encrypted or otherwise secured.

Portable media may not be used without specific permission from the school's Computing Department followed by a virus check. It may not be used off site without encryption.

Staff passwords will be changed regularly.

Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.

Files held on the school's network will be regularly checked by the Computing Manager.

The Computing Manager will review system capacity regularly, which will be documented and filed.

Managing e-mail

Pupils may only use approved EXA-pupilmail e-mail accounts.

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.

Staff only

E-mail sent to external organisations on behalf of the school should be written carefully and Head/Deputy Head informed.

The forwarding of chain letters is not permitted – see code of practice.

E-mail traffic will be monitored by the Computing Manager.

Managing Published Content

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.

E-mail addresses should be published carefully, to avoid spam harvesting.

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

The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Publishing Pupil's images and/or work

Images 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.

Written permission from parents or carers will be obtained before images of pupils are electronically published.

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 and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

Pupils should be advised not to place personal photos on any social network space.

They should consider how public the information is and consider using private areas.

Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.

Teachers' official blogs or wikis should be password protected and run from the school website.

Teachers will not run social network spaces for student use on a personal basis.

Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.

Students should be encouraged to invite known friends only and deny access to others.

Students should be advised not to publish specific and detailed private thoughts.

School should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments. – see *Anti-bullying policy* for further clarification.

The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice following the *Anti-bullying policy* where appropriate.

Filtering

The school will work with EXA, to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL must be reported to the school's ICT.

The Head teacher will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any changes made on this review will be documented and filed.

Any material that the school believes is illegal must be reported to appropriate agencies such as EXA, IWF or CEOP and Unisys by the Network Manager or Head teacher.

The school's filtering strategy will be designed by the EXA in consultation with the Head teacher and Computing Manager to suit the age and curriculum requirements of the pupils, advised by engineers.

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. Mobile phones should be handed in to the school office for safe keeping until the end of the school day. The sending of abusive or inappropriate text messages is forbidden.

The school should investigate wireless communication technologies.

Personal data

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

Authorising Internet access

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

All staff must read and sign the 'Staff Information Systems Code of Conduct' and GDPR Policy 2018 before using any school Computing resource.

Parents will be asked to sign and return a consent form for pupil access.

Parents will be informed that pupils will be provided with supervised Internet access.

Risk Assessment

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Exa can accept liability for the material accessed, or any consequences resulting from Internet use.

The Computing Department in conjunction with the Head teacher should audit Computing use annually to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. Any changes made based on the review will be documented and all staff informed.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Please also consult the school's Computing Code of Practice for further information and clarification.

E-Safety complaints

Complaints of Internet misuse will be dealt with by the Head teacher. Any complaint about staff misuse must be referred to the Head teacher.

Prevent Strategy

As part of St Mary's commitment to safeguarding and child protection we fully support the government's *Prevent Strategy to help build resistance to extremism.*

What is the Prevent Strategy?

The Prevent strategy is a government strategy designed to stop people becoming terrorists or supporting terrorism. It:

- responds to the ideological challenge we face from terrorism and aspects of extremism, and the threat we face from those who promote these views
- provides practical help to prevent people from being drawn into terrorism and ensure they are given appropriate advice and support
- works with a wide range of sectors (including education, criminal justice, faith, charities, online and health)

All members of staff have undertaken Prevent training.

All computing incidents must be reported to the Computing Manager and Head teacher.

Communications Policy

Introducing the Policy to pupils

E-safety rules will be posted in rooms with Internet access.

Pupils will be informed that network and Internet use will be monitored.

An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.

Instruction in responsible and safe use should precede Internet access.

An e-safety module will be included in the PSHE and Computing programmes covering both school and home use.

Staff Discussions

All staff will be given the school e-safety policy and its application and importance explained. Discretion and professional conduct is essential.

Staff that manage filtering systems or monitor Computing use will be supervised by senior management and have clear procedures for reporting issues.

Parents' Support

Parents' attention will be drawn to the school's e-safety policy.

Internet issues will be handled sensitively (ie: children accessing inappropriate websites or using social media platforms in an inappropriate manner) and parents will be informed accordingly.

Approved by the Governing Body: 4th July 2018