Our Lady & St Edwards Catholic Academy

E-Safety Policy Statement

December 2019

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 benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. This will include current new technology and how we should behave when using them.

Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT, bullying and for child protection.

Our e-Safety Policy has been written by the school. It has been agreed by senior management and approved by governors.

 The e-Safety Policy was revised by: Alex Hebbes, December 2019.

 The next review date is (at least annually): January 2021.

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. The school has 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 staff and pupils. Therefore, Internet use will 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.

 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.

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

 Pupils will be taught how to report unpleasant Internet content

 Pupils will be taught about behaviour whilst accessing Internet content.

Managing Internet Access

Information system security

 School ICT systems security will be reviewed regularly.

 Virus protection will be updated regularly.

 Security strategies will be discussed with Frog box 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.

 In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

 Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

 The school should consider how e-mail from pupils to external bodies is presented and controlled.

 The forwarding of chain letters is not permitted.

Published content and the school web site

 Staff or pupil personal contact information will not generally be published.

The contact details given online should be the school office.

Publishing pupil's images and work

 Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children.

 Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.

 Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

 Work can only be published with the permission of the pupil and parents/carers.

 Pupil image file names will not refer to the pupil by name.

 Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic devices.

Social networking and personal publishing

 The school will control access to social networking sites, and consider how to educate pupils in their safe use.

 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, their friends or their location.

 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 when using social networking sites.

Managing filtering

 The school will work with Frogbox IT to ensure systems to protect pupils are reviewed and improved.

 If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.

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

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.

 The senior leadership team should note 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.

 Pupils are not permitted to have mobile phones in class.

 Staff will use a school phone where contact with pupils is required or a school camera will be used to capture photographs of pupils.

Protecting personal data

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

Policy Decisions

Authorising Internet access

 All staff will agree to the Acceptable ICT Use Agreement before using and ICT equipment.

 The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

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

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

Assessing risks

 The school will take 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.

 The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and 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 Head Teacher.

 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 (see complaints policy)

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

Communications Policy

Introducing the e-safety policy to pupils

 e-Safety rules will be discussed with pupils regularly.

 Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

 e-Safety training will be embedded within the ICT scheme of work or the

Personal Social and Health Education (PSHE) curriculum.

 E-safety posters and lessons to be shown/taught to children and parentsabout being safe on the internet.

Staff and the e-Safety policy

 All staff will be given the School e-Safety Policy and its importance explained.

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

 Staff will always use a child friendly safe search engine when accessing the

web with pupils.

Enlisting parents' and carers' support

 Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

 The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.