St Elizabeth's Catholic Primary School
E-Safety Policy

Teaching and Learning

The internet is an essential element in 21st century life for education, business and social interaction. St Elizabeth's 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.

- 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 be 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.
- 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.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will e updated regularly.
- Security strategies will be discussed with the Local Authority.

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 forwarding of chain letters is not permitted.

Published content and the school website

- Staff or pupil personal contact information will not be published. The contact details on the website are those of 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.
- Pupils' full names will not be used anywhere on the school website or other online spaces, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Work can only be published with the permission of the pupil and parents/carers.

Social networking and personal publishing (See Social networking Policy)

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

Managing filtering

- The school will work with MGL technician and LEA to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable online materials, the site must be reported to the e-safety co-ordinator.

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.
- Mobile phones will not be allowed in school.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet Use

- All staff must read and sign the **Staff Acceptable Use Policy** for ICT before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Pupil, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.
- Parents will be asked to sign and return a consent form. (**Pupil Acceptable Use Policy)**

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate materials.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by the ICT co-ordinator and the SLT.
- 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.
- 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 posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and internet use will be monitored and appropriately followed up.

Staff and the e-safety policy

- All staff will be given the school e-safety policy and its importance explained.
- 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 and on the school website.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

Internet use – Teaching and learning activities.

Activities	Key e-safety issues
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved online materials.
Using search engines to access information from a range of websites.	Filtering must be active and checked regularly. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.
Exchanging information with other pupils and asking questions of experts via e-mail or blogs	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information.
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. Staff must ensure that published images do not breach copyright laws.
Communicating ideas within chat rooms or online forums.	Access to social network sites should be blocked. Pupils should never give out personal information.
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. School should only use applications that are managed by Local Authorities and approved Educational Suppliers.