St. Paul's Catholic Primary School

E-Safety Policy

Introduction to E-Safety

1.1 E-Safety in a Changing World

The term E-safety covers the issues relating to young people and staff and their safe use of the Internet, mobile phones and other electronic communication technologies. This policy assesses the protocols for ensuring that these initiatives are carefully developed in our school, so that we progress responsibly and appropriately in the interests of our children. It also looks at how we educate our children to be safe in a world where technology is so readily available.

At St Paul's RC Primary School we celebrate the value and importance of technology in our children's learning. In our school, wireless laptops, iPads, digital voice recorders, camcorders and digital cameras are all part of children's every day learning. The internet has become a vital source of learning and communication for all members of our school community.

Pupils interact with new technologies such as mobile phones and the Internet on a daily basis and experience a wide range of opportunities and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger.

Our school seeks to provide the right balance between controlling access, setting rules and educating both children and parents for responsible use.

Recently we have;

- Purchased 16 iPads and expanded our wireless technology throughout the whole school,
- Launched our Virtual Learning Environment (eSchools) and began to develop use of this,
- Run sessions for children on e-safety;
- Developed teacher expertise in the use of technology within the classroom

This year we have aspirations to:

- Use technology even more to enhance learning experiences,
- Run sessions for parents outlining the importance of e-safety
- Develop each child's awareness of e-safety and use these skills proactively
- Further develop staff knowledge of the 2014 new curriculum.

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

• Education for responsible ICT use by staff and pupils;

• A comprehensive, agreed and implemented e-Safety Policy;

- A well thought out approach regarding how to develop e-Safety guidance within the identified opportunities to ensure that we support families with the challenges relating to school's curriculum;

- E-safety in the digital age (family workshops, web links etc)

- Secure, filtered broadband from the LA

1.2 E-Safety and the Legal Issues

E-safety should be applied to protect children, staff and all members of our school community. Our

School's e-Safety Policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole. e-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally. Anyone can send messages, discuss ideas and publish material with little restriction, although some material is unsuitable for children.

Schools need to protect themselves from legal challenge. The law is catching up with Internet developments: for example it is a criminal offence to store images showing child abuse and to use electronic communications to 'groom' children. In addition there are many grey areas for schools to consider regarding communication through social network sites, storage of data, etc. Schools can help protect themselves by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is unauthorised. The school needs to ensure that all reasonable actions have been taken and measures put in place to protect users. In addition there are many grey areas for schools to consider regarding communication of social network sites, storage of data etc.

In practice this means that this school ensures that;

- It has effective firewalls and filters on our school network.
- Ensures that e-safety responsibilities are clearly communicated to all members of our school community.
- That our Acceptable Use Policies are fully enforced for children, staff and visitors.
- Ensures that our procedures are consistent with the Data Protection Act (1998)

Learning and Teaching in the Digital Age

The school uses wireless laptops and iPads and comprehensive broadband access to develop learning and teaching through digital communication. Access to instant messenger services and mobile phones is not allowed as part of this school's curriculum. However, the school will include provision to educate children how to use this technology appropriately and safely.

2.1 Why the Internet and digital communications are important

Mobile Communication equipment and the Internet are 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. We also recognise that children are actively engaged with digital communication form an early age. It is part of their lifelong learning experiences and habits. Many people of this generation are what Marc Prensky refers to as 'digital natives'. We have to embrace that opportunity. However, we also have a responsibility to ensure that our children learn to use these opportunities and resources responsibly, appropriately and productively to enhance their learning.

In addition, use of the Internet is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2 Encouraging responsible use of the Internet and digital communication.

1. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. This is arranged through local authority provision and the school's network arrangements with RM. Only sites approved by the head teacher will be allowed to override the filter.

2. Pupils will be taught about responsible and appropriate information sharing through the internet and other forms of digital communication.

3. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

4. Pupils will be taught about responsible use of e-mails and other sources of digital communication including e-mail, messenger services and texts.

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

6. Pupils will be shown how to publish and present information to a wider audience safely and responsibly

2.3 Pupils will be taught how to evaluate Internet and other digital communication 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 or other digital content including messages, e-mails and texts. Whilst we cannot promote the use of social networking sites, we must also ensure that our children know how to manage the risks and dangers associated with these activities.

Managing Digital Access, Communication and Content

All Internet accessed is managed by the school. Individual users should only access the Internet through their username and password. The school recognises that password protection is vital element of promoting e-safety.

The school will ensure that permission for access and use of any content including photographs and video is fully explained and sought on admission to the school. It is the responsibility of parents to inform us should they wish to change this during their child's time at St Paul's

3.1 Information system security

- School ICT systems security will be reviewed regularly. This will be part of the liaison between the head teacher and Wirral's Technical Services department.
-
- Virus protection will be updated regularly as part of the school's Service Level Agreement with the Local Authority.

- Security strategies will be discussed with the Local Authority.

3.2 Managing filtering

- The school will work with Wirral Local Authority and other National Bodies 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 Miss Newton.

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

3.4 Published content and the school web site/social media

• Staff or pupil personal contact information will not be published. The contact details given online should be the school office or a senior member of staff.

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

3.5 Publishing pupil's images and work

• Photographs that include pupils will be selected carefully, and will not include images of pupils where parents have not signed the general consent form. This is to ensure that individual pupils cannot be identified or their image misused. The school will always risk assess photographs for possible abuse.

• Names or any other personal details will never be published alongside photographs.

• Pupils' full names will not be used anywhere on a school VLE 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 repositories Guidance @ Children, Families, Health and Education Directorate page 6 June 2008.

3.6 Social networking and personal publishing

• The school will control access to social networking sites, and consider how to educate pupils in their safe use. The school considers that this should be carefully managed. All staff will seek the approval of the head teacher before using any such site.

- Newsgroups will be blocked unless a specific use is approved.

• Appropriate e-safety lessons are completed by pupils to advise them:

  - never to give out personal details of any kind which may identify them, their friends or their location.
  - that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
  - to use nicknames and avatars when using social networking sites.

This guidance is applied through the Local Authority's policy on the agreed use of social networking sites and the school's acceptable use and E-Safety code of conduct. All staff and visitors including students have to sign these when they join our staff team.

3.7 Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security. Video conferencing for pupils can only take place under the direct supervision of a member of staff. At St Paul's RC Primary we will only use webcams for specific projects and full consent will be sought before children participate in these. Examples may be conferencing with another school in France,

- All software for webcam use will be password protected (Skype etc).

- Best practice recommends that schools always seek consent from parents for any videoconferencing

3.8 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. For example, children are not allowed to bring mobile devices to school.

- Staff are allowed to have mobile devices in school but these must not be used during working hours except for school or emergency based communication in office areas or the staffroom. All mobile devices should be stored securely in the admin block during school hours.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

- The use by pupils of cameras in mobile phones is not allowed.

- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

- Staff will be issued with a school phone where contact with pupils is required. Staff have been given digital cameras and must not take photographs on their personal phones.

- Guidance @ Children, Families, Health and Education Directorate page 7 June 2008

3.9 Protecting personal data

• Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. This information will be clearly communicated to all staff, including office staff on an annual basis.

Staff are aware that they have a professional responsibility to ensure the following;

- All laptops must be password protected. Work laptops cannot be used for the storage of any inappropriate material.
- Photographs in Drop Box should only be accessed in school and should be moved into the school media storage folder and deleted from the device also.
- All data and images of children must be stored in the staff shared area on the curriculum network or the school's secure administration network.
- Photographs cannot be stored on personal laptops.

3.10 Use of Photographs

The Data Protection Act 1998 affects our use of photography. This is because an image of a child is personal data for the purpose of the Act and it is a requirement that consent is obtained from the parent of a child or young person under the age of 18 years (or the child him or herself if deemed competent from 12 years old as suggested by the Information Commissioner) for any photographs or video recordings for

purposes beyond the school's core educational function. (E.g. school web sites, school productions). At St Paul's RC Primary we seek permission for all photography and video use.

There will also be times where the school will be carrying out off-site activities e.g. activity holidays or educational visits. Our guidelines are created to make sure that all images are taken appropriately by both adults in the school and children taking part in visits.

For both, school setting and other events which are photographed for publicity purposes, additional consent should be sought from the child's parent/guardian or the child and kept on file covering all cases where images of children are to be published beyond the parameters of school use.

Where children are "Looked After" schools must check consent on the corporate parent's behalf with the social worker and there may be other situations, (in adoption placements or following a resettlement from domestic violence for example), where a child"s security is known by the class teacher to be at stake, indicating the need for extra care.

Consent gained for photographs or videos may not extend to webcam use, so it is important to check, when introducing such technology, the status of existing consent for pupils or models.

Developing Policy on E-safety

The pace of change with emerging technology means that all staff have to be vigilant about risks concerned with e-safety. School Policy has to be proactive and clear.

The responsibility for ensuring the effective implementation of e-safety policies is the head teacher's. Individual members of staff have responsibilities under their pay and conditions to ensure that these policies are followed. Clear advice is issued by professional organisations such as the NUT, NAHT, UNISON etc on these matters.

The Governing Body will consider these matters. Many duties will be devolved to the Health and Safety Committee. The Governing Body will exercise their duty to ask the head teacher to consider any matters arising from policy reviews.

4.1 Authorising Internet access

- All staff must read and sign the Policy on the use of social networking websites before using any school ICT resource.

- All Parents/Carers will be asked to sign and return the general consent form on entry to school which gives permission for their child to access the internet under supervision

- Any person not directly employed by the authority will be asked to sign an "acceptable use of school ICT resources" before being allowed to access the internet from the school site.

4.2 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. Within school pupils are

trained to shield themselves from unsuitable material and to report such material to a member of staff who will identify the site and take steps to block this via the local authority.

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.

4.3 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 safeguarding nature must be dealt with in accordance with school safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Discussions will be held with the Police Youth Crime Officer to establish procedures for handling potentially illegal issues.

4.4 Community use of the network and Internet

Through extended schools use and partnership with other organisations there may be wider community use of the school's network. The school will liaise with local groups to establish a common approach to e-safety

Communicating the E-Safety Policy

5.1 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.

• A programme of training in e-Safety has been developed, based on the thinkyouknow resources.

• E-Safety training will be embedded within the ICT scheme of work

5.2 Staff and the e-Safety policy

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

• Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

• 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 suitable search engine when accessing the web with pupils.

5.3 Enlisting parents' and carers' support

• Parents' and carers' attention on the school Virtual Learning Environment.

• The school will maintain a list of e-safety resources for parents/carers on request and can provide technical support to support their child's safe use of the Internet.

• The school will ask all new parents to sign the general consent form when they register their child with the school.