Saint Peter's Catholic Primary School

'Christ in the centre, excellence at the heart'

Mission Statement

To provide a	**C**atholic Education, embracing world faiths,
Nurturing	**H**appy and motivated children
Who want to	**R**each to achieve high expectations
	In partnership with parents
	Supported by a committed staff and Governing Body
Who help children	**T**o feel self-worth and know success

E-SAFETY / ACCEPTABLE USE POLICY

Approving Committee:	Curriculum, Inclusion & Standards	
Approved /Adopted Date:	05/02/18	Meeting Minutes of: 05/02/18
Signed:	John Cullinan	(Chair of approving/adopting committee)
Name:	John Cullinan	
Next Review Date:	Spring 2019	

The St Peter's Schools e-Safety policy provides details of procedures to be followed relating to e-safety issues and links to further information.

It is revised regularly in line with the Governing Body's policy review.

This policy covers the safe use of internet and electronic communications technologies such as mobile phones and wireless connectivity. The policy highlights the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It also provides safeguards and rules to guide staff, pupils and visitors in their online experiences.

The school's e-safety policy operates in conjunction with others including policies for Behaviour, Curriculum, Data Protection, Child Protection, Safeguarding Children, plus the Home-School Agreement and Anti-bullying.

Effective Practice in e-Safety

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

- All internet technologies & electronic communications such as mobile phones, Facebook etc
- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband;
- A school network that complies with the National Education Network standards and specifications.

2.1 Teaching and learning

2.1.1 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.
- Enhanced teaching and learning.

2.1.3 Internet use will enhance learning

- The school Internet access has been designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are shown how to publish and present information to a wider audience.
- Pupils' use is monitored by adults at all times. There are sanctions for misuse in line with th Governing Body's Behaviour policy.

2.1.4 Pupils will be taught how to evaluate Internet content

- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught the importance of cross-checking information before accepting its accuracy.
- Pupils are taught how to report misuse/abuse or offensive material through Internet Safety Week.

2.2 Managing Internet Access

2.2.1 Information system security

- School ICT systems security is reviewed regularly and monitored by ICT Technician/ICT Co-ordinator.

- Virus protection is updated regularly.
- Security strategies are discussed with the Senior Management Team.

2.2.2 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 is treated as suspicious and attachments not opened unless the author is known.
- The school e-mail from pupils to external bodies is presented and controlled by teaching staff.
- The forwarding of chain letters is not permitted.

2.2.3 Published content and the school web site

- Staff or pupil personal contact information is not published. The contact details given online will be the school office.
- The headteacher & ICT Technician take overall editorial responsibility and ensure that content is accurate and appropriate.

2.2.4 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 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 do not refer to the pupil by name. especially when used as content for the school website or social media accounts.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

2.2.5 Social networking and personal publishing

- The school controls access to social networking sites, and educates pupils in their safe use.
- Newsgroups are blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils are advised to use nicknames and avatars when using social networking sites.
- All school staff are regularly advised of the professional and personal risks associated with the use of social networks, including private facilities.
- All school staff will ensure their social networking sites are not accessible by pupils. Staff are advised of the risks associated with linked content and posts made by others in exposing their accounts to pupils.
- Pupils are helped to develop critical thinking skills to reflect and enable them to keep themselves safe.

2.2.6 Managing filtering

- The school works to ensure pupils are protected from unsuitable websites.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator or Headteacher.

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

2.2.7 Managing videoconferencing & webcam use

Currently not in use.

2.2.8 Managing emerging technologies

- Emerging technologies are examined for educational benefit and risk assessments are carried out before use in school is allowed.
- The senior leadership team are aware 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.
- Pupil's mobile phones should be handed into the office. 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. Mobile phones should not be used at the school disco.
- 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 are issued with a school phone and school camera where contact with pupils is required or where mobile phones are used to capture photographs of pupils.
- The appropriate use of Learning Platforms is discussed as the technology becomes available within the school.
- No photographs are taken on staff's personal phones or cameras.

2.2.9 Protecting personal data

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

2.3 Policy Decisions

2.3.1 Authorising Internet access

- All staff must read and sign the Staff Code of Conduct for ICT before using any school ICT resource.
- The school maintains a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet is by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents are asked to sign and return a consent form. (See appendix to ICT policy).
- All children are under adult supervision whilst using computers.

2.3.2 Assessing risks

- The school takes 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. Neither the school nor Leicestershire Local Authority can accept liability for any material accessed, or any consequences of internet access.
- The school audits ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective. (See appendix iii).

2.3.3 Handling e-safety complaints

- Staff must not communicate with pupils (past or present) via social networking sites.
- Staff will ensure their social networking sites are not accessible by pupils.

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- 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's Safeguarding procedures.
- Pupils and parents are informed of the complaints procedure (see schools complaints policy).
- Pupils and parents are informed of consequences for pupils misusing the internet, usually detention after school.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.
- Complaints of cyberbullying will be dealt with in accordance with the Anti-bullying policy.
- Any e-safety issue will be logged.

2.3.4 Community use of the Internet

- The school liaises with local organisations to establish a common approach to e-safety.

2.4 Communications Policy

2.4.1 Introducing the e-safety policy to pupils

- e-safety rules are posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils are informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed, possibly based on the materials from CEOP (see appendix iv for exemplar teaching and learning activities).
- e-Safety training is embedded within the ICT scheme of work and the Personal Social and Health Citizenship Education (PSHCE) curriculum.

2.4.2 Staff and the e-Safety policy

- All staff are given access to the School e-Safety Policy and its importance explained.
- Staff are informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use are supervised by senior management and work to clear procedures for reporting issues.
- Staff always use a child friendly safe search engine when accessing the web with pupils.

2.4.3 Enlisting parents' and carers' support

- Parents' and carers' attentions are drawn to the School e-Safety Policy in Newsletters, policies can be requested from the school website.
- The school has annual e-safety awareness evenings for parents.
- The school asks all new parents to sign the parent /pupil agreement when they register their child with the school.

This policy was approved by the Governing Body on 05/02/18 and will be reviewed in Spring 2019.

Signed by (Name) John Cullinan Date 05/02/18

Signature John Cullinan Designated Position Chair of CIS

Appendix iii e-Safety Audit – Primary

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Many staff could contribute to the audit including: SENCO, e-Safety Coordinator and Network Manager.

Has the school an e-Safety Policy? Y/N

Date of latest update:

The school e-safety policy was agreed by governors on:

The policy is available for staff at:

The policy is available for parents/carers at:

The responsible member of the Senior Leadership Team is:

The responsible member of the Governing Body is:

The Designated Child Protection Coordinator is:

The e-Safety Coordinator is:

Has e-safety training been provided for both pupils and staff? Y/N

Is there a clear procedure for a response to an incident of concern? Y/N

Have e-safety materials from CEOP been obtained? Y/N

Do all staff sign a Code of Conduct for ICT on appointment? Y/N

Are all pupils aware of the School's e-Safety Rules? Y/N

Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils? Y/N

Do parents/carers sign and return an agreement that their child will comply with the School e-Safety Rules? Y/N

Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced? Y/N

Has an ICT security audit been initiated by SMT, possibly using external expertise? Y/N

Is personal data collected, stored and used according to the principles of the Data Protection Act? Y/N

Is Internet access provided by an approved Internet service provider which is deemed safe & secure for pupils to use? Y/N

Has the school-level filtering been designed to reflect educational objectives and approved by SMT? Y/N

Appendix 2

Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I will not store images of children on personal phones, cameras or laptops.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I will not allow children to use the computers without proper adult supervision.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.
- I will not communicate with pupils via email, IM and social networking sites.
- I will ensure my social network sites are not accessible by pupils.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: …… Capitals: …… Date: ……

Accepted for school: …… Capitals: ……