eSafety Policy

St Peters Catholic Primary School

Mission Statement: *Through loving God, everyone at St Peter's school is committed to creating a happy, loving and secure environment for learning, which has Christ at the heart of its community, where everyone is valued, included and shows respect for each other.*

Developing and Reviewing this Policy

This eSafety Policy has been written as part of a consultation process involving the following people:

Staff, Governors and Lancashire advisors.

It has been approved by Governors and will be monitored and reviewed as listed below:

Policy Created - Date: July 2011

The implementation of this policy will be monitored by: Head Teacher, Governors

This policy will be reviewed as appropriate by ICT subject leader/Head teacher

Approved by …… (Headteacher) Date ……

Approved by …….. (Governor) Date ……

Contents

eSafety Policy 2010 St Peters Catholic Primary School

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective eSafety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our eSafety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

2. Our school's vision for eSafety

At St Peter's, we use technology when appropriate to enhance the learning experience for our children and to support the daily organisation and administration tasks carried out by school staff.

Keeping members of our school community safe, whilst using technology, is a priority and we expect staff to act as role models in their use of technology and abide by the shared decisions reflected in our eSafety policy. Children are encouraged to explore and make responsible decisions regarding their uses of technology, informed by 'education' as opposed to the imposition of restrictions. As children are engaging with 21st Century technologies both inside and outside of school, we will provide opportunities for both children, staff and parents to understand and view eSafety education as a key life skill.

Our eSafety Policy defines what we consider to be acceptable and unacceptable behaviour regarding the uses of technology in school and the sanctions or procedures to be followed should breaches of security occur. It is communicated to staff, governors, pupils and parents and is updated in light of the introduction of new technologies or incidents.

3. The role of the school's eSafety Champion

It is recommended that schools have an eSafety Champion, usually nominated from the Senior Leadership Team, but this will vary according to individual school settings, phases and needs. For more details regarding the role and responsibilities of the eSafety Champion, see section 3 (The role of the school's eSafety Champion) in the Lancashire safety guidance document. In this section of your policy, you may want to specify a named person and outline the core duties of this role.

Our eSafety Champion is
Mrs E Kelly

The role of the eSafety Champion in our school includes:

- to keep a log of incidents an ensure staff are aware of reporting procedures and requirements should a safety incident occur.
- to ensure that the policy is implemented and that compliance with the policy is actively monitored.

Delegated duties to ICT leader:

- to keep up to date with safety issues and guidance through the Local Authority Schools' ICT Team and through advice given by national agencies. (i.e. CEOP, Child Exploitation)
- Ensure the Head teacher, SLT, staff, pupils and governors are updated as necessary.
- To be responsible for e Safety advice/training for staff, parents/carers and governors

4. Policies and practices

This eSafety policy should be read in conjunction with the following other related policies and documents:

- **Safeguarding**
- **Safe practices at work**

4.1 Security and data management

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

- Key information / data is mapped and securely stored on the main office computer. This is accessible only by the bursar and head teacher.
- The head teacher has overall responsibility for managing all information.
- Staff have been informed of the location of all data relevant to them by the head teacher.
- Staff have been informed of their legal responsibilities with respect to principles of the Data Protection Act (1988) and ensure all data is :
    1. Accurate
    2. Secure
    3. Fairly and lawfully processed
    4. Processed for limited purposes
    5. Processed in accordance with the data subject's rights
    6. Adequate, relevant6 and not excessive
    7. Kept no longer than necessary
    8. Only transferred to others with adequate protection

Our school ensures that data is appropriately managed both within and outside the school in the following ways:

- School 's equipment , including teacher laptops, must only be used for school purposes and do not contain personal information eg, personal images, personal financial details, music downloads, personal software. Computers are accessed via a safe username and password and it is the responsibility of the individual to keep this secure at all times. Any breaches in security must be reported immediately to (named person).
- School equipment must not be used, for example for online gambling, dating websites home shopping, booking holidays, social networking BOTH at home and in school.
- Staff are aware of the school's procedures for disposing of sensitive data, eg, shredding hard copies, deleting digital information, deleting usernames and passwords from school's VLE, deleting email accounts, IEP, PIPs, SATs information and know the person responsible should there be any queries.
- The school ensures all data is removed prior to disposal or repair of equipment and all staff are aware of the person responsible.
- Remote access is available to SLT and they are only allowed to access data from home via a secured wireless connection. School data must NOT be stored on personal equipment, eg, home computer or mobile phone.
- Staff are advised not to use personal storage devices, eg, external hard drives, pen drives, mobile phones on school equipment.
- Member of staff (where needed) will be provided with an encrypted, password protected device to use on school equipment when it is necessary to store data highly confidential information as part of their professional role. All staff have access to a personal storage space within My LGfL and the staff category in Moodle and should use this as the preferred area for backing up data.

4.2 Use of mobile devices

In our school we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

- No electronic equipment is permitted to be brought into school**.**
- Any visitors will be asked to turn their mobile devices off whilst in the school.

Please see AUP for staff, parents and children for further guidance.

4.3 Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

- **Permission is gained through the children's AUP which is done yearly. (see appendix 4)**
- **Additional permission for digital images is gained through Image consent form, (see appendix 1), which includes retention once the child has left school.**
- **No photographs will contain a child's full name, first name only will be used and on videos – children refer to each other by first names only.**
- **Parents and visitors are allowed at certain times to take digital images of children but they are reminded at every event that these are for personal use and must not be shared electronically in any way.**
- **All photos and video taken in school are taken using school equipment where possible or using a school SD card in a personal camera.**
- **All photos/video must be saved onto safe area of the cloud or teacher's computer and immediately deleted from the camera so no image is stored on the equipment.**
- **Photographs/videos are stored centrally on a pass word protected part of the cloud, or on a teacher's computer behind a password so only authorised personnel are able to access them.**
- **All staff, parents, children and visitors are aware that no image of pupils or staff can be published on the internet in any form without the permission of the person involved.**
- **ICT leader/ head teacher will monitor implementation of safe practice relating to the use of digital media, as outlined in this policy.**

See appendix 1 AUP Image consent.

4.4 Communication technologies

As a school we understand the importance of communication and the role it plays in today's society and endeavour to educate and protect the children our care.

Email:

In our school the following statements reflect our practice in the use of email.

- All users may only use approved e-mail accounts on the school system.
- Pupils and staff must immediately report an offensive, threatening or bullying in nature e-mail to their teacher or eSafety champion.
- No inappropriate information should be included in emails and a disclaimer attached to the bottom of the email.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- All users must be made aware that all email communications may be monitored at any time in accordance with the AUP and Telecommunications Regulations 2000

Social Networks:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

- The school will not give access to social networking sites, but consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- All users will be advised never to give out personal details of any kind which may identify them, their friends/colleges or their location.
- If adults use a social network site then details must not be shared with pupils both past and present, and privacy settings be set at maximum.
- All users must conduct themselves on these sites in a professional manner and not publish any thing that could bring the schools name into disrepute.

Mobile telephone:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Mobile telephones:

- No mobile phones are permitted to be brought into school by the children**.**
- Any visitors will be asked to turn their mobile devices off whilst in the school.
- Staff have phones turned off during teaching time and must ensure no children are present during their break times when using their phone.
- If a child needs to bring a mobile phone for the journey to and from school it is handed in to the class teacher who sends it in a box to be stored in the office until school has ended.

Instant Messaging:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Instant Messaging:

- Staff and children in school cannot access this service due to Lancashire filtering service.
- Within school these sites are blocked but guidance will be given, through teaching on the Moodle, on how to use them safely.

Virtual Learning Environment (VLE) / Learning Platform:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Virtual Learning Environments:

- All children and staff have access to the school Moodle through passwords set for their need of use. The pupils have access to the courses, teachers as administrators on the courses and ICT leader and Head teacher as administrators for the Moodle.
- Pupils are taught through the curriculum how to access work, chat rooms and discussion forums in a responsible way within curriculum time.
- ICT leader/technician will add/delete users who join/leave school.
- Teaches have responsibility for monitoring their tear groups chat/discussion groups to maintain responsible practices. ICT leader and Head teacher have overall responsibility for monitoring teachers.

Web sites and other online publications

In our school the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

- **The filtering for web sites is devolved to Lancs ngfl under the net sweeper filter.**
- There are attachments on the school website for parents and visitors outlining safe internet use.
- All members of staff and children are aware of the guidance for digital media and personal information on the website.
- The head teacher and ICT technician have access to the website to edit content and keep the information up to date. The head teacher has overall responsibility for the content of the schools website
- All users are aware of copyright restrictions including personal intellectual copyright and will not publish anything that does not meet this.
- Any file available for download is in PDF file to eliminate manipulation and redistribution without consent.

Video conferencing:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing:

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

Others:

As new technologies are introduced this policy will be adapted/updated to take account of them and any associated risks.

4.5 Acceptable Use Policy (AUP)

Our school has AUP's for teaching staff and governors, pupils and supply/visitors. See appendices 1-4

4.6 Dealing with incidents

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Head teacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF).

Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.

It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. The head teacher or designated safety champion will always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk) .They are licensed to investigate – schools are not!

Any incident in your classroom must be reported to the safety champion and recorded in the log. We understand that there are 2 types of incident illegal and inappropriate and how we should respond to each.

The table below outlines possible incidents, procedures and sanctions:

Incident Procedure and Sanctions	**Incident Procedure and Sanctions**
Accidental access to inappropriate materials.	• Minimize the webpage/turn the monitor off/click the „Hector Protector" button. • Tell a trusted adult. • Enter the details in the Incident Log and report to LGfL filtering services if necessary. • Persistent „accidental" offenders may need further disciplinary action.
Using other people' s logins and passwords maliciously.	• Inform SLT or designated eSafety Champion. • Enter the details in the Incident Log. • Additional awareness raising of eSafety issues and the AUP with an individual child/class. • More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy.
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate	

way.	• Consider parent/carer involvement.

- Children are made aware of the procedures during safety sessions and reminded each time before accessing online material
- Any incidents are logged on the incident log in the head teachers office which is monitored by the head teacher termly.
- If an incident occurs their understanding and suitability of access will be assessed to see if it is safe for that individual to use.
- Parents/external agencies are only involved with repeated incidents or when individuals are not under appropriate levels or supervision.
- See safety incident/escalation procedures appendix 9-10

5. Infrastructure and technology

Pupil Access: children are only allowed to use school equipment when directed by a trusted adult. They are only allowed to access online material with the supervision of a trusted adult.

Passwords: our network does not need password access. All Moodle users have passwords which are kept within Moodle and only the head teacher and ICT subject leader have access to these. Children and staff are reminded of keeping them secure hen ever they use them. Passwords will only be changed if the user looses or forgets their password by the designated people.

Software/hardware: all our software is licensed or free to download/use. The licenses are held in the head teacher's office and they are the nominated person responsible for keeping those up to date.

Equipment used and software are audited yearly and new ones purchased or removed as needed by the ICT technician/ICT subject leader/ head. They also have responsibility for installation of software onto school systems.

Managing the network and technical support: We work from a link station and the network is not a server. All devices that access the wireless management system have security enabled and can only be accessed with the schools wireless network password. All computers are set to automatically update important software, particularly protection software.

The Head teacher then ICT subject leader is ultimately responsible for managing the security of the school network.

Users are allowed to download software with the permission of the ICT subject leader/head teacher who ensures correct licences are there or covered under present licences.

The ICT technician is monitored by the ICT subject leader and head teacher who liaise with them every visit. They are aware of the schools safety standards and requirements and meet these.

Staff use encrypted pen drives to ensure security of data and use individual laptops but nothing is saved onto the laptop.

Filtering and virus protection: Our school uses the LGfL filtering service for any online activity. If there is a particular problem with a site or the need to unblock a site then the head teacher will liaise with LGfL to try to remedy the problem. Virus protection is supplied by Sophos in conjunction with LGfL. Staff laptops must be brought into school once a month and their virus protection software updated to ensure most recent version is installed.

6. Education and Training

6.1eSafety across the curriculum

As a school our approach to learning is through a creative curriculum that uses strong cross curricular links between subjects. We see eSafety as reaching across all subjects and is therefore addressed initially through ICT and PSHE but then reinforced through all the other subjects. From 2011-2012 we are hoping to have in place specific eSafety sessions relating to the year groups to help children understand how to stay safe on equipment they night be using.

6.2eSafety – Raising staff awareness

Staff have read and discuss eSafety policy as a staff. Training is followed up on particular areas highlighted by individuals by the ICT subject leader in conjunction with e safety champion and any appropriate out side agencies like CEOP and the police. Any trainers will have received training through Lancashire/CEOP. Their training will involve any issues related to their own safety and children's safety. All staff will promote and model responsible use of ICT and digital resources. All staff new to school is inducted with the current up to date eSafety information and acceptable use policy so they have a good understanding of what is acceptable and not.

6.3eSafety – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

Our school has an area of the website and Moodle for parents with links to site that will inform them and support them in guiding their children with eSafety while at home. There are also updates sent home in the weekly news letter when needed to remind parents as well as yearly parents safety awareness sessions held by Police, CEOP trained members of staff and other appropriate outside agencies.

6.4eSafety – Raising Governors' awareness

The governors are aware of the eSafety policy and all it entails. They have read and signed the acceptable use policy concerning them (see appendix 2). They will be updated with current practices and training when appropriate at governors meetings.

7 Standards and inspection

- We will monitor the incident log each term and deal with any serious incidents immediately as review the policy every 2 years or when new technology is introduced.
- ESafety incidents are recorded in the log in head teachers office, which is then reviewed and monitored by esafety champion.
- The introduction of new technologies will be risk assessed and added to the safety policy at earliest opportunity.
- All incidents will be analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children by head teacher/eSafety champion and procedures/training adapted to take account.
- These patterns be addressed using the most effective method e.g. working with a specific group, class assemblies and parents newsletters.
- Any incidents recorded will be reviewed and may cause adaptations to be made to the eSafety policy by ICT subject leader/safety champion.
- Staff, parents/carers, pupils and governors are informed of changes to policy and practice through the AUP's done yearly and changed ones sent out when needed during the year. All people involved information as soon as possible once changes have been made.