

ST PETER'S CHURCH OF ENGLAND PRIMARY SCHOOL

E-Safety Policy September 2016

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at St Peter's we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

E-safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for St Peter's School.

“As in any other area of life, children and young people are vulnerable and may expose themselves to danger – knowingly or unknowingly – when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly legal... To ignore e-safety issues could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable.”
From: Safeguarding Children in a Digital World. BECTA 2006

Our e-safety Policy has been written by the school, following government guidance. It has been agreed by teachers, senior leaders and approved by governors.

- The school's e-safety coordinators are the 'Computing team'.
- The Designated Safeguarding Leads – Mrs A Martin and Mrs S Knox
- The e-safety Governor is Mrs Amanda Care
- The e-safety Policy and its implementation shall be reviewed annually
- It was approved by the Governors on 6th October 2016 and will be reviewed in the Autumn Term 2017 as part of our safeguarding review

Roles and Responsibilities

Governors

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. The role of the e-Safety Governor will include:

- Receive a termly update form the e-Safety Co-ordinator during the Strategic Development Committee Meeting
- Regular monitoring of e-Safety incident logs
- Reporting to the full Governing Body termly

Headteacher (who is the e-Safety Co-ordinator)

- The Headteacher is responsible for ensuring the safety (including e-Safety) of members of the school community

- The Headteacher is responsible for ensuring that all relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train others colleagues, as relevant
- The HEadteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The HEadteacher should be aware if the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff
- The Headteacher will take day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents
- The Headteacher ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- The Headteacher liaises with the Deputy Headteacher who co-ordinates training for staff
- The Headteacher liaises with school ICT technical staff and the Deputy Headteacher who is the strategic lead for ICT
- The Headteacher receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

Teaching and Learning

The internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed expressly for pupil use including appropriate content filtering
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- As part of the ICT (computing) curriculum, all year groups will have opportunities to focus on different elements of staying safe online. This will include topics such as how to use a search engine, digital footprints and cyber bullying
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through meetings with our SEN co-ordinators and individual teachers to ensure all children have equal access to succeeding in this subject.

Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information.

Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to e-safety and agree to its use:

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource
- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access (within the Home-School Agreement)
- Only authorised equipment, software and Internet access can be used within the school

World Wide Web

The Internet opens up new opportunities and is now an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time, and content shall be reported to the teacher who will then report to the Headteacher, by recording the incident in an e-Safety Log, which will be stored in the Headteacher's office with other safeguarding materials. The e-Safety Log will be reviewed termly by the Headteacher and e-Safety Governor. Impero
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the material by staff and pupils complies with copyright law.
- The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

E-mail

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of e-Safety:

- Pupils may only use approved e-mail accounts on the school system
- Pupils must immediately tell a teacher if they receive offensive e-mail
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Access in school to external organisations should be written carefully and authorised before sending, in the same way as using outlook
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff log-on. Staff must always log-out of a PC if they are going to leave it unattended, even for a short period of time e.g. breaktime

Social Networking

- Use of social networking sites and newsgroups in the school is not allowed and will be blocked/filtered
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils
- Pupils will be encouraged to only interact with known friends and family over the Internet and deny access to others
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber-bullying and defamatory comments.

Reporting

All breaches of the e-safety policy need to be recorded in the e-Safety reporting book that is kept in the Headteacher's office (locked filing cabinet behind the door). The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to one of the Designated Leads immediately (Headteacher or Deputy Headteacher). It is their responsibility to decide on appropriate action not the class teachers.

Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to the Headteacher on the same day.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff.' If necessary, the Local Authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, Childline)

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of image. There are risks of mobile bullying, or inappropriate contact.

- Pupils are not permitted to bring mobile phones onto the school premises
- Staff should always use the school land-line phones to contact parents
- All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the day
- Staff may use their mobile phones in the staffroom/one of the school offices
- Parents cannot use mobile phones on school trips to take pictures of the children

Digital/Video Cameras/Photographs

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'
- Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background
- The Headteacher or a nominee will inform parent(s)/carer(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner

Staff should always use a school camera to capture images and should not use their personal devices. Photos taken by the school are subject to the Data Protection act.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents

- Contact details on the Website will be the school address, e-mail and telephone number
- Staff and pupils' personal information will not be published
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate
- Photographs and videos that include pupils will be selected carefully
- Pupils' full name will not be used in association with photographs
- Consent from parents will be obtained before photographs of pupils are published on the school website
- Work will only be published with the permission of the pupil
- Parents should only upload pictures of their own child/ children onto social networking sites

- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with the Local Authority
- E-safety will be discussed with our ICT support and those arrangements incorporated in to our agreement with them

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate

Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by the Headteacher
- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature shall be dealt with in accordance with the school child protection procedures
- Pupils and parents will be informed of the complaints procedure
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues

Communication of Policy

Pupils:

- Pupils will be informed that their Internet use will be monitored
- Pupils will be informed of the importance of being safe online. This will be strongly reinforced across all year groups during ICT lessons and all year groups look at different areas of safety through the computing curriculum

Staff:

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

Parents:

- Parents attention will be drawn to the School e-Safety Policy in newsletters and on the school website

Further Resources

We have found these websites useful for e-Safety advice and information.

http://www.thinkuknow.co.uk	Set up by the police with lots of information for parents and staff including a place to report abuse
http://www.childnet-int.org	Non-profit organisation working with others to 'help make the Internet a great and safe place for children'