ST.PAUL'S
CHURCH OF ENGLAND
PRIMARY SCHOOL

ENGAGE – INSPIRE - ACHIEVE

The Christian family of St Paul's… moving forward together. A caring, exciting and happy school where everyone succeeds!

Online Safety Policy January 2020

Mission Statement

The family of St Paul's CE Primary School work together to create a caring, stimulating and happy school environment, in which each individual can develop to his/her fullest potential within the context of Christian values.

Links to other policies

Computing Policy. Acceptable Use Policy Staff. Home and School Agreement.

AIMS AND PRINCIPLES

A School's Online Policy must cover 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 Online Safety Policy will operate in conjunction with others including policies for behaviour, Anti - Bullying, Data Protection, Children Protection, Security Policy and the Home-School Agreement.

Effective Practice in Online 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;
Secure, filtered broadband from the Lancashire County Council;
A school network that complies with the National Education Network standards and specifications

Writing and reviewing the Online Safety Policy

The Online Policy is part of the School Development Plan and relates to other policies including those for Computing, bullying and for child protection.
The school has appointed an Online Safety Coordinator. This is the Designated Child Protection Coordinator as the roles overlap. It is not a technical role.
Our Online Safety Policy has been written by the School, building on the LCC e-Safety guidance. It has been agreed by senior management and approved by governors.

1. Teaching and learning

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.

2. Internet use will enhance learning

- 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 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
- Pupils will be shown how to publish and present information to a wider audience.

3. Pupils will be taught how to evaluate Internet 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 content by informing a member of staff.

4. Managing Internet Access - Information system security

School ICT systems security will be reviewed regularly.
Virus protection will be updated regularly.
Security strategies will be discussed with the ICT Consultant in conjunction with Local Authority.
Access to internet sites is managed through Netsweeper as installed by Lancashire.

E-mail (where appropriate)

- 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 school should consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

5. Published content and the school web site

- Staff or pupil personal contact information will not be published.
- The contact details given online will be the school address, telephone and email.
- The Head teacher and individual content managers will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with school's guidelines for the publications, including respect for intellectual property rights and copyright.
- The content of the website will be regularly reviewed and updated according to current government and Ofsted guidance.

6. 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 a 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 will not refer to the pupil by name.
- A register of children without consent will be kept by the e-Safety Officer and their images will not be published in accordance with the parent's wishes.
- Images and video must be captured using school devices only. All images of children must be stored securely on the school network.

Part taken out here about 'Child Media Policy'.

7. Social networking and personal publishing (where appropriate)

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Pupils will not be allowed to access conventional social networking sites (Facebook, MySpace, Ask.fm, Bebo etc).
- Newsgroups will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. Pupils will be advised to use nicknames and avatars when using social networking sites.

8. Managing filtering

The school will work with the Local Authority and Westfield 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 Online Safety Coordinator.
- The ICT Consultant will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Violations will be reported to the Computing Lead in the first instance and subsequently to the Principal.
- Access to internet sites is managed through Netsweeper as installed by Lancashire.

- A ‘report an e-safety concern’ button is present on the children’s desktops, and can be completed by any child.

9. Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Teachers must ask permission from the Computing lead/Head before making or answering a videoconference call.
- Videoconferencing and webcam use will be appropriately supervised for the pupil’s age.

10. 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

- Mobile phones will not be used by staff or pupils during lessons, except by prior arrangement with the Principal.
- The sending of abusive or inappropriate text messages or files by Bluetooth, WiFi or any other means is forbidden.
- Pupils are not allowed to use personal mobile phones or devices in school time. Pupils are required to hand their mobile phones and personal devices into the school office at the start of the day. This Policy will be reviewed regularly.
- Personal mobile phones will not be used to capture images of children.
- Violations will be reported to the Head.

11. GDPR - Data Protection Act 2018

The school is registered with the relevant Data Protection authority. It will ensure that it adheres to the Data Protection Act. It will ensure that data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept longer than necessary
- processed in accordance with the data subjects rights
- secure
- not transferred to other countries without adequate protection

12. Authorising Internet access

- All staff must read the Staff Code of Conduct 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.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site.

13. 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.
- The school should audit ICT use regularly to establish if the Online Safety Policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

14. Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a Unit Head.
- 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 (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

15. Staff and the Online Safety Policy

- All staff will be given the School Online 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 child friendly safe search engine when accessing the web with pupils.

16. Introducing the Policy to the children and families

- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- Online Safety training is embedded within the ICT scheme of work.
- Parents and carers attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school Web site.

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

POLICY REVIEW

The Online Safety Policy will be reviewed annually as part of the overall Safeguarding and Child Protection Policy review.

This policy will be ratified by the Governing Body in January 2020

Signed by Mr W Aitkin (Chair of Governors) Date: January 2020

This policy will be reviewed on or before the following date: January 2021

Appendix 1: Useful resources for teachers
BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/
Becta
http://schools.becta.org.uk/index.php?section=is
Chat Danger
www.chatdanger.com/
Child Exploitation and Online Protection Centre
www.ceop.gov.uk/
Childnet
www.childnet-int.org/
Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen
www.digizen.org/
Kidsmart
www.kidsmart.org.uk/
Think U Know
www.thinkuknow.co.uk/
Safer Children in the Digital World www.dfes.gov.uk/byronreview/

Appendix 2: Useful resources for parents
Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
Childnet International "Know It All" CD
http://publications.teachernet.gov.uk
Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk
Parents Centre
www.parentscentre.gov.uk
Internet Safety Zone
www.internetsafetyzone.com

We are a Rights Respecting School. The United Nations Convention on the Rights of the Child (UNCRC) is at the heart of everything we do. The UNCRC articles which are particularly relevant to this policy are:


Children's Rights - Article 19
Every child has the right to be protected from all forms of violence, abuse and neglect.


Children's Rights - Article 28
Every child has the right to an education.