ST.PAUL'S
CHURCH OF ENGLAND
PRIMARY SCHOOL

ENCOURAGE
one another
AND BUILD EACH OTHER UP
1 THESSALONIANS 5:11

Online Safety Policy February 2022

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.

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 Online Safety guidance. It has been agreed by senior management and approved by governors.

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, Social Media Policy, Anti - Bullying, Data Protection, Children Protection, Security Policy and the Home-School Agreement.

Effective Practice in Online Safety

Online 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 Online Safety Policy
Secure, filtered broadband from the Lancashire County Council
A school network that complies with the National Education Network standards and specifications

Rationale

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.

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.
- The use of the internet is to enhance pupils learning and enrich experiences.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Staff will direct pupils to safe sites.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are only given access to the internet when permitted and supervised.
- Pupils will be shown how to publish and present information to a wider audience.
- Pupils regularly receive Online Safety lessons. These are planned for every half term. All children also take part in Internet Safety week.

2. 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.
- Filtering systems are in place and regularly checked.

3. Managing Internet Access - Information system security

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

4.E-mail (where appropriate)

- Pupils may only use approved e-mail accounts on the school system (via Purple Mash).
- 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

- Work can only be published with the permission of the pupil and parents/carers.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. This also includes the use of our ‘PTA Facebook Page’ and ‘Twitter’.
- 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 our school Website or other on-line space, particularly in association with photographs.
- Pupil image file names will not refer to the pupil by name.
- A register of children without consent will be kept by the Online 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.

EYFS -

Pupil’s images and work

- Written permission from parents or carers will be obtained before photographs of pupils are used within the 2 Simple program 2BuildaProfile.
- Any information uploaded to 2BuildaProfile is coherent with GDPR permissions and outlines.
- Written permission is obtained for use of images within children’s learning journey.
- Any other children in images will only be named by their first name.

See Appendix Five.

Using Resources

- EYFS children use the internet via trusted learning platforms i.e. Purple Mash and Spelling Shed.
- EYFS children do not use Google/conduct live searches.
- EYFS children have half-termly Online Safety lessons using age appropriate materials.

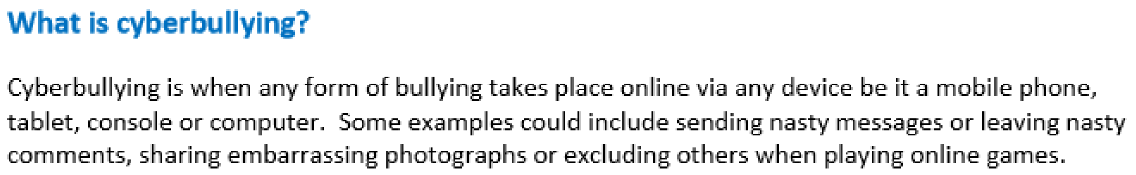
7. Social networking and personal publishing (where appropriate)

- 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. Cyberbullying

Defined (taken from our online newsletter re Cyberbullying)



What is cyberbullying?

Cyberbullying is when any form of bullying takes place online via any device be it a mobile phone, tablet, console or computer. Some examples could include sending nasty messages or leaving nasty comments, sharing embarrassing photographs or excluding others when playing online games.

Preventing and addressing

- School will actively discuss cyber-bullying and we will ensure that children are aware of the effects that this can have on others. Children will also be actively aware of how to report an incident. This will happen within targeted PSHE lessons and Online Safety lessons.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- The school also communicates with parents so that they are aware of the signs, how to report it and how they can support children who may be affected. This is done via our 'Online Safety' page on our school website https://stpaulsrawtenstall.co.uk/Online Safety/ (Appendix 1)
- In relation to a specific incident of cyberbullying the DSL will be responsible for deciding whether an incident needs to be reported to the police or if they need to engage with external services.

Examining and storing students' devices

All children that have a mobile/electronic device are required by school to drop it off of at the office before school starts. These can then be collected after school. Children are not allowed access to personal devices throughout the day.

School have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the DSL to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation (Appendix Two).

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school Complaints Policy and Procedure.

9. Managing filtering

The school will work with the Local Authority and Western Computing Systems 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 Online Safety concern' button is present on the children's desktops and can be completed by any child.

10. Managing New 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 Headteacher.
- 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.

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.

11. Copyright

- All software used within school has an up to date and appropriate license.
- School will ensure that internet scoured materials comply with copyright law.
- School does not state ownership of any materials that have been taken form other sites etc.

12. 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

13. Authorising Internet access

- All staff must read the Staff Code of Conduct/Acceptable Use Policy 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.

14. 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 Online Safety policy is appropriate and effective.

15. Handling Online 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.

16. 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.
- Staff read and are supported by relevant Government Guidelines. Teaching Online Safety in Primary Schools.

17. Children/Families and the Online Safety Policy.

- 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 (see Appendix Three).
- The school has an online 'Online Safety Page' (Appendix One). This is shared with parents via online platforms such as out PTA Facebook Page and Twitter.
- The school publishes a monthly 'Online Safety Newsletter' via our 'Online Safety Page' (Appendix One)

See Appendix 6: Useful sites for Parents.

Article 27:

Every child has the right to food, water, clothing and a safe place to live and learn.

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 February 2022

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

This policy will be reviewed on or before the following date: February 2023

Appendix 1:

Access to our 'Online Safety page'

https://stpaulsrawtenstall.co.uk/Online Safety/

Appendix 2:

Searching, screening and confiscation Advice for headteachers, school staff and governing bodies January 2018

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674416/Searching_screening_and_confiscation.pdf

Appendix 3:

INTERNET ACCESS

The Internet is becoming increasingly important to the way we gather information, communicate with people across the world, work and live.

We believe that the Internet has a contribution to make to your son/daughter's education. In order for your son/daughter to make use of the school's internet facilities we need you to give your permission by signing the 'Internet Permission' section.

We would like to take this opportunity to briefly explain some of the steps we have taken to protect our young people from the inappropriate material that does exist on the Internet.

- The School connects to the Internet through an Internet Service Provider (ISP) that provides a level of protection from inappropriate material by blocking sites that are known to contain materials that would be offensive to the majority of people
- The school has its own filtering software in place that is tailored to the specific needs of our school. This software is regularly updated

- During lessons, teachers will direct pupils to appropriate Internet material that has been visited beforehand
- The school's email facility checks messages coming in and out of the school for inappropriate language, images and viruses
- Internet activities are closely supervised and pupils are not allowed access to computers linked to the Internet unless in the presence of a member of staff
- Pupils are taught acceptable behaviour on the Internet and are asked to agree and conform to our Acceptable Use Policy (AUP)

The school, with support of the LEA, has made every effort to protect our young people from inappropriate material. We believe that the education advantages of using the Internet are enormous and various projects have shown the educational benefits of Internet access.

PROCEDURES FOR DEALING WITH USERS WHO DELIBERATELY MISUSE THE INTERNET

The acceptable behaviour of all members of the school community is covered by existing rules of conduct. In the case of pupils, these will be within the school rules and in the case of staff are contained in their conditions of service.
The internet offers an unusual opportunity for unacceptable behaviour in school.
This could include:

- Cyberbullying
- Actively searching for inappropriate material, including material of a pornographic, racist or violent nature
- Downloading files without permission
- Infringing copyright
- Playing online games
- Attacking another person's web sites
- Sending bullying emails/SMS text messages to mobiles

Using unauthorised Chat rooms, Bulletin Boards, User Groups or other areas of the Internet.

The school should consider appropriate sanctions, for example:

- Temporary or permeant ban on Internet use
- Disciplinary action in line with existing practices and conditions of service

In extreme circumstances the LEA and or/police may need to be involved.

Misuse of the school's facility may not only break the school's rules but may also contravene one or more of the following:

The obscenity Acts of 1959 and 1964- The Protection of Children Act 1978

The Indecent Display Act of 1981- The Criminal Justice Act 1988

The Copyright, Designs and Patents Act 1988- The Obscene Publication Act 1989

The Data Protection Act 1998- The Computer Misuse Act 1990

ICT ACCEPTABLE USE POLICY

These rules reflect the content of our school's eSafety Policy. It is important that parents/carers read and discuss the following statements with their child/ren understanding and agreeing to follow the school rules on using ICT, including the use of the Internet.

- I will only use ICT in school for school purposes
- I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher
- I will only use the Internet and/or online tools when a trusted adult is present
- I will only use my class email address or my own school email address when emailing
- I will not deliberately look for, save or send anything that could be unpleasant or inappropriate
- I will not deliberately look for, or access inappropriate websites
- If I accidently find anything inappropriate, I will tell my teacher immediately
- I will only communicate online with people a trusted adult has approved
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not give out my own, or other's details such as names, phone numbers or home addresses
- I will not tell other people my ICT passwords
- I will not arrange to meet anyone I have met online
- I will not access any of my files from home or delete any in school
- I will not attempt to download or install anything on to the school network without permission
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my eSafety
- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy

We have discussed this Acceptable Use Policy and _______________ (print child's name) agrees to follow the Online Safety rules and to support the safe use of ICT at St Paul's Primary School.

Parent/Carer Name (Print) ____

Parent/Carer Name (Print) ____

Date ____

This AUP must be signed and returned before any access to school systems is allowed.

This form is valid from the date you sign it for a period of 7 years or for the time your child attends this school, whichever is sooner. The consent will automatically expire after your child has left this school. Should you wish to make any changes to your consent, you will need to contact the school office and complete another consent form.

Appendix 4:

Teaching Online Safety in Schools

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf

Appendix 5:

2SIMPLE - ONLINE LEARNING JOURNEY

Within our EYFS unit your child's learning will be recorded through photographs and observational notes by all staff within the unit using 2Simple software. I agree to the school storing this information on the 2Simple app.

Child's Name:	
Signed (Parent/Carer):	
Name of Parent/Carer:	
Date:	
Email address:	

Appendix 6: Useful sites for Parents

Access to our ‘Online Safety page’

https://stpaulsrawtenstall.co.uk/Online Safety/

Action Fraud: www.actionfraud.police.uk
BBC WebWise: www.bbc.co.uk/webwise
CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
ChildLine: www.childline.org.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
Know the Net: www.knowthenet.org.uk
National Online Safety: www.nationalonlinesafety.com
Net Aware: www.net-aware.org.uk
NSPCC: www.nspcc.org.uk/onlinesafety
NSPCC/O2 Online Safety: www.nspcc.org.uk/preventing-abuse/keeping-children-safe/onlinOnline Safety/
Parent Port: www.parentport.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/
Think U Know: www.thinkuknow.co.uk
Virtual Global Taskforce: www.virtualglobaltaskforce.com
Vodaphone Digital Parenting: www.vodaphonedigitalparenting.co.uk
UK Safer Internet Centre: www.saferinternet.org.uk
360 Safe Self-Review tool for schools: https://360safe.org.uk/