St Paul's Church of England Primary School Oswaldtwistle

'Don't let anyone look down on you because you are young but set an example for the believers in speech; in conduct; in love; in faith and in purity (1 Timothy 4:12).'

Online Safeguarding Policy

September 2024
Agreed by Governors:

Overview

Online Safeguarding encompasses the safeguarding of children when using internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

This policy has been written by the school, building on government guidance; it operates in conjunction with other policies including those for Computing, Behaviour, Anti-Bullying, Curriculum, and Safeguarding & Child Protection. The school's Designated Senior Leader takes overall responsibility for Online Safeguarding at school.

Why Using Technology is Important

Technology and the internet are 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 and use of other technologies are a part of the statutory curriculum and a necessary tool for staff and pupils. Pupils use a variety of technology widely outside school and need to learn how to evaluate information and to take care of their own safety and security. The school will aim to create resilient and sensible technology users who can assess risks independently.

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 will be given clear objectives for internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval, filter and evaluation. Pupils in Reception-Year 4 are not permitted to 'free-surf' the web. Internet access for these pupils will be achieved by staff providing a selection of evaluated sites

The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Information System Security and filtering

School ICT systems capacity and security will be reviewed and monitored regularly with both the ICT technician and subject lead. Important findings will be fed back to SLT and any concerns found from reviewing and monitoring will be reported to the DSL. Virus protection will be updated regularly as required.

Managing Filtering

The school will work with the LA, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the Head teacher, the Online Safety Lead and logged via CPOMS. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that the school believes is inappropriate will be reported to appropriate agencies. The internet filtering system will be regularly assessed and if found to be unsuitable will be updated as a priority. Schools can assess as high, medium or low risk in regard to the need to filter internet content. As a school, we have risk assessed ourselves to be of medium risk as children sometimes use devices without direct supervision and we know our children use a range of technologies and are aware children know of and use a number of websites which could have inappropriate content. Due to this assessment, we will ensure filtering is monitored on a monthly basis.

Published content, School Website & School Facebook Page

Contact details on the website/Facebook page should be the school address, e-mail and telephone number. Staff, Governor or pupils' personal information will not be published. The Headteacher takes overall editorial responsibility and ensures that content is accurate and appropriate. The Headteacher, Computing lead and Bursar are the only staff permitted to have access to the school's Facebook log in. Staff will ensure any information published on the school website or Facebook page demonstrate our Christian vision and shows we behave appropriately in school and we set examples in 'speech; in conduct; in love; in faith and in purity' (1 Timothy 4:12)

Publishing Pupil Images

Photographs that include pupils will be selected carefully. Pupils' full names will not be used anywhere on the Website/Facebook page or in association with photographs. Written permission from parents/carers will be obtained on the pupil's entry to school, before photographs of pupils are published online. Parents/carers will be notified at all public performances about the guidelines for confidential use of images in respect of social networking sites.

Social Networking and Personal Publishing

The school will block/filter access to social networking sites. Through regular online safety lessons, pupils will be advised never to give out personal details of any kind which may identify them or their location.

Pupils and parents/carers will be advised that the use of social network spaces such as Facebook outside of school is against the law for primary aged pupils. They will also be advised of the benefits and dangers of other social networking/gaming platforms aimed at primary school aged children. They will also be offered specific guidance, through online safety workshops, National College Guides and items on the newsletter on how they can best keep their children safe should they permit use at home.

Managing Video Conferencing

IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the internet. Pupils are not permitted engage in video conferencing outside of a planned lesson and under the supervision of staff. The use of Microsoft Teams and Zoom is by staff members. Video conferencing will be appropriately supervised for the pupils' age.

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. Mobile phones should not be brought into school by pupils and will not be used during lessons or formal school time. If mobile phones need to be in school, e.g. for children walking home, they must be handed to the office at the start of the school day. If found during the school day, mobile phones belonging to pupils will be handed to the headteacher and parents will be contacted.

Teachers will contact parents using a text message service when the need occurs e.g. school closures, cancellation of after school activities, reminders about meetings and events. Parents should not contact staff through text messaging.

Protecting personal data

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

Authorising Internet access

All staff must read and sign the Acceptable Usage Agreement (AUP) before using any school ICT resource. The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave, or a pupil's access be withdrawn. Parents/carers will be given a copy of the AUP which governs ICT use in school as their child enters school. All pupils will be required to read, understand and sign the 'St. Paul's Acceptable Use Policy' each year as part of Online Safety lessons and a copy of this will be displayed in all classrooms.

Assessing risks

The school will take all reasonable precautions to ensure that users are safe and access only appropriate material, and there is appropriate and substantial filtering software in place to ensure that pupils do not access material linked to terrorism, extremism or of a sexual nature. 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 school computer. Neither the school nor LA can accept liability for the material accessed, or any consequences of internet access. We will work with parents to support in the use of technology at home and we provide regular training and updates through posters and newsletters regarding popular sites and apps children are using.

The school will audit ICT provision to establish if the Online Safeguarding policy is adequate and that its implementation is effective. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

Staff will monitor and log any online safety worries with children via CPOMs using the online safety category. Staff and governors will continue to have both safeguarding training and regular online safety training. 'Keeping children safe in education 2024' states: - "Schools/colleges should recognise that child-on-child abuse, including sexual violence and sexual harassment can occur online. School/colleges have an essential role to play in both preventing online child-on-child abuse and responding to any concerns when they occur, even if they take place offsite and should have appropriate systems in place to support and evidence this." Staff are aware of the potential risks in regard to child-on-child bulling and staff will record any incidences of online bullying and follow the school's behavioural policy in dealing with any incidences.

In line with "Keeping Children Safe in Education 2021" staff are aware that "children who are victims of sexual violence and sexual harassment will likely find the experience stressful and distressing. This will, in all likelihood, adversely affect their educational attainment." Staff understand that it is important that all victims of sexual violence, harassment and other forms of online abuse are "taken seriously and offered appropriate support." Staff will log any concerns about victims using CPOMs and the school's pupil support worker and SLT will work closely with victims, their families and appropriate agencies to offer appropriate support.

Further to this, guidance from The Church of England Education Office in "Valuing All God's Children" states that 'Opportunities should be offered for pupils to explore why some people seek to bully and how bullying can take the form of homophobic, biphobic or transphobic bullying. Strategies about how to protect yourself and others from bullying should be taught including online safety.' Following from this guidance, pupils will explicitly be taught how to recognise forms of online bullying and will be encouraged to speak to a trusted adult if they are aware of any forms of online bullying. Children will be encouraged to act online how they would in life and follow our vision through setting an example 'in speech; in conduct; in love; in faith and in purity' (1 Timothy 4:12)

Reporting Online Safety Incidents

All staff will monitor and log Online Safety incidents via CPOMS using the Online Safety category. These will include any discussions with pupils regarding apps, devices, games and websites that they have viewed at home. These incident reports will then be used to inform the actions of the Online Safety group and the work of the Online Safety Champions.

Monitoring and Intervention

An Online Safety Group comprising of representatives from the SLT, the Online Safety Lead and the Pupil Support Worker will meet each half term to collate and discuss the online safety incidents reported via CPOMS. Intervention and support will be planned in these meetings to support individual/groups of pupils and their families.

Pupil representatives (Online Safety Champions) will meet with the Online Safety Lead regularly to share their experiences of pupils across school. The group will act as ambassadors for Online Safety and lead events in school that support and develop our pupils understanding of Online Safety.

Handling Online Safety Complaints

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 safeguarding/child protection nature must be dealt with in accordance with school safeguarding/child protection procedures (see safeguarding policy). Parents and pupils will need to work in partnership with staff to resolve issues.

Introducing the Online Safeguarding Policy to Pupils

Online Safety rules will be discussed with the pupils at the start of each year. Pupils will be informed that network and internet use will be monitored. Pupils in all classes will receive specific online safety lessons using Project Evolve. Pupils will be expected to adhere to the AUP and pupils will be required to read, understand and sign the AUP each year as part of Online Safety lessons.

Staff and the Online Safeguarding Policy

All staff will be expected to read the school's Online Safeguarding Policy as part of induction, and then annually (or when updates are made) as part of the school's Safeguarding Policy and Guidance suite. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential. Staff training in safe and responsible internet use and on the school Online Safeguarding policy will be provided as required.

Parents/Carers

Parent/carers' attention will be drawn to the School Online Safeguarding Policy in newsletters and on the school website at regular intervals throughout the school year. Internet issues will be handled sensitively, and parents/carers will be advised accordingly. The school website contains safe search website links for children to conduct digital research on at home and parents have been advised to download the National Online Safety App to keep themselves up to date on Online Safety at home.

Reviewed: September2024
Review Date: September 2026

St. Paul's Primary School
Acceptable Use Policy for Staff and Governors

The computer systems owned by the school are made available to staff, pupils and community learners to support and enhance education. Equipment provided for staff remains school property.

St. Paul's School will endeavour, wherever possible, to provide a safe and secure environment for its users. However, please be aware that we cannot guarantee complete safety from inappropriate material. The responsibility must also lie with each individual to use ICT in a safe, sensible and responsible way.
When using technology I agree to:

Use only my own login, passwords and user names and keep these secret.
Never access technology using someone else's login, password or username without permission.
Never purposefully access or distribute material which may be considered offensive to others (this includes, racist, abusive, indecent material).
Close down any offensive material and report it immediately to the technician.
Never access sites which are unrelated to work e.g. internet shopping, whilst in working time/hours.
Never enter anyone else's, including the school's, personal information on the internet.
Never purposefully access inappropriate internet sites.
Be polite, respectful and friendly to those I contact through technology.
Report any unpleasant messages sent to me or accessed by me accidentally. I understand my report would be confidential
Never use technology in a way which would be damaging or derogatory to the school, or staffs, reputation. This includes making comments about the school and staff outside of school premises using social networking sites, chat rooms, Youtube, Twitter and text messages.
Never to accept pupils (past or present) as friends on social networking sites.
Never to use digital photographs of other members of staff on social networking sites, websites or other public technology without their permission.
Never to install software without first discussing with the ICT technician. This applies to teacher laptops used at home.
Not access and use copy written material without having the correct licences in place.
Never use mobile phones while directly in charge of pupils.
Remote Learning: • Students are set work that is accessible, engaging and relevant • Learning activity instructions are clear and precise • To apply the highest level of privacy settings for Learning platforms and Zoom • All lessons on Zoom to have encrypted invites, unique meeting IDs and secure passwords

I understand that violating any of the above could result in my temporarily being unable to use school technology and in severe cases could result in disciplinary proceedings. In extreme cases, the police will be informed and criminal prosecution may follow.

Name: **Signature:** **Date:**

Acceptable Use Policy Key Stage 1 and EYFS

St Paul's Technology Promise

When using technology in school we will:

- Take care when carrying equipment
- Ask before going online.
- Tell an adult if something goes wrong or upsets me
- Think before I click.
- Only use my own passwords and log ins.

We understand that if we do not behave correctly with technology, we may not be allowed to use technology in school. All the children in year _____ agree to this.

Signed by the teacher: _____

Acceptable Use Policy Key Stage 1 and EYFS

St Paul's Acceptable Use Policy

When using technology in school we will:

- Take care when carrying equipment.
- Ask before going online.
- Speak kindly to others when emailing or sending other messages.
- Tell an adult if something goes wrong or upsets me.
- Think before I click.
- Only use my own passwords and log ins.

We understand that if we do not behave correctly with technology, we may not be allowed to use technology in school. All the children in year _____ agree to this.

Signed by the teacher: _____