



St Peter's Catholic Primary School



Policy	Online Safety Policy and Procedure v2
Date Approved/Approving Body:	25.10.23
Signed – Chair of Governors:	L Murphy
Date of Next Review:	October 2025

'Loved by Jesus, we love, we learn, we live and grow together for Him'

Contents:

Statement of intent

1. [Legal Framework](#)
2. [Teaching and learning](#)
3. [Managing internet access](#)
4. [Publishing pupils' images and work](#)
5. [Policy decisions](#)
6. [Pupil online safety curriculum](#)
7. [Communications policy](#)
8. [Remote Learning](#)
9. [Online Hoaxes and harmful online challenges](#)
10. [Educating Parents](#)

Appendices

- a) [Online safety Activities and Issues](#)
- b) [Useful Resources for Teachers and Parents](#)
- c) [Response to an Incident of Concern Flowchart](#)
- d) [Staff, Governor and Visitor Acceptable Use Agreement](#)
- e) [Acceptable Use Agreement: Pupils](#)
- f) [Rules for EYFS and KS1](#)
- g) [Rules for KS2](#)

Statement of intent

Protecting young people and adults properly means thinking beyond the school environment. Broadband, Wi-Fi and 3/4/5G connections now mean the world wide web is available anywhere, anytime. Moreover, the introduction of the internet on games consoles, tablets and mobile phones mean it is becoming increasingly difficult to safeguard our children from the dangers hidden in cyberspace.

Our children will not only be working online in school or at home; their personal devices are not always covered by network protection and it is, therefore, imperative that they are educated on the risks involved with using the internet and are provided with guidance and a range of strategies on how to act if they see, hear or read something that makes them feel uncomfortable.

As a result, designing and implementing an Online Safety Policy demands the involvement of a wide range of interest groups: the governors, headteacher, SLT, SENCO, DSL, classroom teachers, support staff, young people or parents, LA/Academy personnel, internet service providers (ISP), and regional broadband consortia, working closely with ISPs on network security measures.

Online safety is a child protection issue, and indeed it should not be managed primarily by the ICT team. It should be an extension of general safeguarding and led by the same people, so that, for instance, cyber bullying is considered alongside real-world bullying.

An Online Safety Policy should:

- Allow young people to develop their own protection strategies for when adult supervision and technological protection are not available.
- Give information on where to seek help and how to report incidents.
- Help young people understand that they are not accountable for the actions that others may force upon them but that there are sanctions that the school will impose if they act inappropriately when online.
- Provide guidelines for parents and others on safe practice.
- Ensure you regularly monitor and review your policies with stakeholders.
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective online safety program.

Above all, online safety education should be a continuing feature of both staff development and young people's educational lifelong learning.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at school with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of the school.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behavior and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.

- Have clear structures to deal with online abuse, such as online bullying, which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behavior, is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupil.

1. Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2021) 'Keeping children safe in education 2020'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

2. Teaching and learning

Why the internet and digital communications are important

- 2.1. 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.
- 2.2. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- 2.3. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- 2.4. Staff model safe and responsible behaviour in their use of technology during lessons.
- 2.5. Teachers remind pupils about their responsibilities through an end-user [Pupil Acceptable Use Agreement](#) which every pupil will sign when they log on to the school network.

Internet use will enhance learning

- 2.6. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- 2.7. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- 2.8. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- 2.9. Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate internet content

- 2.10. The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- 2.11. Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- 2.12. Pupils will be taught how to report unpleasant internet content to the online safety coordinator. This can be done anonymously, or in person, and will be treated in confidence.
- 2.13. The school has a clear, progressive online safety education programme as part of the computing curriculum and half termly digital literacy sessions. This covers a range of skills and behaviours appropriate to their age and experience, including:
 - To STOP and THINK before they CLICK.
 - To develop a range of strategies to evaluate and verify information before accepting its accuracy.
 - To be aware that the author of a website/page may have a bias or purpose and to develop skills to recognise what that may be.
 - To know how to narrow down or refine a search.
 - To understand how search engines work and to understand that this affects the results they see at the top of the listings.
 - To understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
 - To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
 - To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.
 - To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos, and to know how to ensure they have turned-on privacy settings.
 - To understand why they must not post pictures or videos of others without their permission.
 - To know not to download any files – such as music files – without permission.
 - To have strategies for dealing with receipt of inappropriate materials.
 - To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
 - To know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

3. Managing internet access

Information system security

- 3.1. School ICT systems security will be reviewed regularly.
- 3.2. Virus protection will be updated regularly.
- 3.3. Security strategies will be discussed with the LA.

Email

- 3.4. Pupils may only use approved email accounts on the school system.
- 3.5. Pupils must immediately tell a teacher if they receive an offensive email.
- 3.6. In email communication, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.
- 3.7. Incoming emails will be treated as suspicious and attachments not opened unless the author is known.
- 3.8. The school will consider how emails from pupils to external bodies are presented and controlled.
- 3.9. The forwarding of chain letters is not permitted.
- 3.10. The school:
 - Provides staff with an email account for their professional use (BGFL 365) and makes clear personal email should be through a separate account.
 - Does not publish personal email addresses of pupils or staff on the school website.
 - Will contact the police if one of our staff or pupils receives an email that it considers is particularly disturbing or breaks the law.
 - Will ensure that email accounts are maintained and up-to-date.
 - Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the police.
 - Knows that spam, phishing and virus attachments can make emails dangerous.

Published content and the school website

- 3.11. Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- 3.12. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate, and the quality of presentation is maintained.
- 3.13. Uploading of information is restricted to our website authorisers.
- 3.14. The school website complies with the following statutory DfE guidelines for publications:
 - [What maintained schools must publish online](#)
- 3.15. The point of contact on the website is the school address and telephone number. The school uses a general email contact address, enquiry@stjonfsh.bham.sch.uk. Home information or individual email identities will not be published.
- 3.16. Photographs published on the web do not have full names attached.
- 3.17. The school does not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

4. Publishing pupils' images and work

- 4.1. Photographs that include pupils will be selected carefully so that individual pupils cannot be identified, or their image misused. The school will consider using group photographs rather than full-face photos of individual children.
- 4.2. Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs.
- 4.3. Written permission from parents will be obtained before photographs of pupils are published on the school website.
- 4.4. Work can only be published with the permission of the pupil and parents.
- 4.5. Pupil image file names will not refer to the pupil by name.
- 4.6. Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
- 4.7. The school gains parental permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school.
- 4.8. Staff sign the school's [Staff, Governor and Visitor Acceptable Use Agreement](#), and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- 4.9. The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- 4.10. Pupils are taught about how images can be manipulated in their online safety education programme and to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.
- 4.11. Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- 4.12. Pupils are taught that they should not post images or videos of others without their permission. The school teaches them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. The school teaches them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Social networking and personal publishing

- 4.13. The school filtering system blocks access to social networking sites
- 4.14. Newsgroups will be blocked unless a specific use is approved.
- 4.15. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- 4.16. Staff will be reminded of the risks of accepting parents and children as 'friends' on social networking sites, will be strongly advised not to do so, and given advice on how to 'block' children from viewing their private pages.
- 4.17. Staff will be encouraged to 'untag' themselves from any inappropriate pictures that may appear on social networking sites.
- 4.18. School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or LA.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Managing filtering

- 4.19. If staff or pupils come across unsuitable online materials, the site must be reported to the online safety coordinator.
- 4.20. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing and webcam use

- 4.21. Videoconferencing should use the educational broadband network to ensure quality of service and security.
- 4.22. Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- 4.23. Videoconferencing and webcam use will be appropriately supervised.

Managing emerging technologies

- 4.24. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- 4.25. The SLT 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.
- 4.26. Mobile phones will not be used during school time.
- 4.27. Staff will not use personal mobile phones to communicate with children or use them to capture images of them.

Protecting personal data

- 4.28. Personal data will be recorded, processed, transferred and made available according to the GDPR and the Data Protection Act 2018.

Personal devices, wearable technology and mobile phones

- 4.29. The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored and recorded.
- 4.30. The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of this procedure.
- 4.31. Where parents or pupils need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times. Mobile phones will not be used during lessons or formal school time.

- 4.32. Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or on silent at all times.
- 4.33. Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- 4.34. Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. the staff room.
- 4.35. No images or videos should be taken on mobile phones or personally-owned mobile devices
- 4.36. Staff handheld devices, including mobile phones and personal cameras, must be noted in school – name, make and model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- 4.37. Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- 4.38. Staff will be issued with a school phone where contact with pupils' parents is required.
- 4.39. Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods, unless permission has been granted by a member of the SLT in emergency circumstances.
- 4.40. Staff will not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- 4.41. If a member of staff breaches the school policy, disciplinary action may be taken.
- 4.42. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- 4.43. Pupils will abide by the following rules when using personal devices in school:
- The school strongly advises that pupil mobile phones should not be brought into school; however, we accept that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety. Phones are collected in at the start of the school day and returned at home time for older children who may choose to walk home.
 - If a pupil needs to contact their parents, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the **school office**.
 - Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in the safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

5. Policy decisions

Authorising internet access

- 5.1. All staff will read and sign the [Staff, Governor and Visitor Acceptable Use Agreement](#) before using any school ICT resource.
- 5.2. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- 5.3. At EYFS and KS1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.
- 5.4. Any person not directly employed by the school will be asked to sign the [Staff, Governor and Visitor Acceptable Use Agreement](#) before being allowed to access the internet from the school site.

Assessing risks

- 5.5. 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. Neither the school nor the LA can accept liability for any material accessed, or any consequences of internet access.
- 5.6. The school should audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

Handling online safety complaints

- 5.7. Complaints of internet misuse will be dealt with by a senior member of staff.
- 5.8. Any complaint about staff misuse must be referred to the headteacher.
- 5.9. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- 5.10. Pupils and parents will be informed of the complaints procedure (see school's complaints policy)
- 5.11. Pupils and parents will be informed of the consequences for pupils misusing the internet.
- 5.12. Discussions will be held with the police youth crime reduction officer to establish procedures for handling potentially illegal issues.

6. Pupil online safety curriculum

Teaching and learning

- 6.1. This school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to the age of the children, including:
 - To STOP and THINK before they CLICK.
 - To develop a range of strategies to evaluate and verify information before accepting its accuracy.
 - To know how to narrow down or refine a search.
 - To understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.

- To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.
 - To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
 - To have strategies for dealing with receipt of inappropriate materials.
 - To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
 - To know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.
- 6.2. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- 6.3. The school will remind pupils about their responsibilities through a [Pupil Acceptable Use Agreement](#) which every pupil will sign.
- 6.4. All staff will model safe and responsible behaviour in their own use of technology during lessons.

Online risks

- 6.5. The school recognises that pupils increasingly use a range of technology such as mobile phones, tablets, games consoles and computers. It will support and enable children to use these technologies for entertainment and education but will also teach children (in PSHE) that some adults and young people will use such outlets to harm children.

Cyber bullying and abuse

- 6.6. Cyber bullying can be defined as "Any form of bullying which takes place online or through smartphones and tablets." - BullyingUK
- 6.7. Complaints of online bullying are dealt with in accordance with our **Anti-Bullying Policy**. Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.
- 6.8. Through the PSHE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails or text messages.
- 6.9. Cyber bullying will be treated as seriously as any other form of bullying and will be managed through our anti-bullying and confiscation procedures. Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- 6.10. All incidents of cyber bullying reported to the school will be recorded.

Sexual exploitation/sexting

- 6.11. Sexting between pupils will be managed through our anti-bullying and confiscation procedures.

- 6.12. All staff are made aware of the indicators of sexual exploitation and all concerns are reported immediately to the DSL.
- 6.13. There are clear procedures in place to support anyone in the school community affected by sexting.
- 6.14. All incidents of sexting reported to the school will be recorded.

Radicalisation or extremism

- 6.15. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.
- 6.16. Extremism is defined by the Crown Prosecution Service as “The demonstration of unacceptable behaviour by using any means or medium to express views which:
 - Encourage, justify or glorify terrorist violence in furtherance of beliefs.
 - Seek to provoke others to terrorist acts.
 - Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
 - Foster hatred which might lead to inter-community violence in the UK.”
- 6.17. The school understands that there is no such thing as a “typical extremist”: those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.
- 6.18. The school understands that pupils may become susceptible to radicalisation through a range of social, personal and environmental factors – it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff can recognise those vulnerabilities.
- 6.19. Staff will maintain and apply a good understanding of the relevant guidance to prevent pupils from becoming involved in terrorism.
- 6.20. The school will monitor its RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.
- 6.21. Senior leaders will raise awareness within the school about the safeguarding processes relating to protecting pupils from radicalisation and involvement in terrorism.

7. Communications policy

Introducing the Online Safety Policy to pupils

- 7.1. Online safety rules and guidance posters will be displayed in communal spaces and discussed with pupils regularly.
- 7.2. Pupils will be informed that network and internet use will be monitored and appropriately followed up.
- 7.3. A programme of training in online safety will be delivered through our digital literacy sessions.
- 7.4. Safety training will be embedded within the computing and RHE schemes of work in line with national curriculum expectations.

Staff and the online safety policy

- 7.5. All staff will be given the school Online Safety Policy and have its importance explained.
- 7.6. Staff must be informed that network and internet traffic can be monitored and traced to the individual user.
- 7.7. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- 7.8. Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' support

- Parents' attention will be drawn to the school Online Safety Policy in workshops, newsletters, the school prospectus and on the school website.
- The school will maintain a list of online safety resources for parents.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.
- The school will have a page on its website dedicated to keeping children safe online. It will provide parents with useful links to help them in understanding the internet.

8. Remote Learning

- 8.1 All remote learning is delivered in line with the school's Remote Learning Policy.
- 8.2 All staff and pupils using video communication must:
 - Communicate in groups – no one-to-one sessions will be carried out
 - Wear suitable clothing – this includes others in their household.
 - Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
 - Use appropriate language – this includes others in their household.
 - Maintain the standard of behaviour expected in school.
 - Use the necessary equipment and computer programs as intended.
 - Not record, store, or distribute video material without permission.
 - Ensure they have a stable connection to avoid disruption to lessons.
 - Always remain aware that they are visible and sometimes can be heard.
- 8.3 The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.
- 8.4 The school will consult with parents via the school website/school app about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.
- 8.5 The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections and can recover lost work.
- 8.6 During the period of remote learning, the school will maintain regular contact with parents to:
 - Reinforce the importance of children staying safe online.

- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

8.7 The school will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school. The school will not be responsible for providing access to the internet off the school premises but will however assist families with appropriate resources.

9. Online hoaxes and harmful online challenges

- 9.1. For the purposes of this policy, an **“online hoax”** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.
- 9.2. For the purposes of this policy, **“harmful online challenges”** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.
- 9.3. The DSL and Computing Lead ensures that pupils are taught about how to critically identify when online content is untrue or harmful and how to respond to this content.
- 9.4. The DSL will work with the SENDCO to assess whether some pupils, e.g. pupils who have been identified as being vulnerable or pupils with SEND, need additional help with identifying harmful online challenges and hoaxes, and tailor support accordingly.
- 9.5. The school will ensure all pupils are aware of who to report concerns to surrounding potentially harmful online challenges or hoaxes, e.g. by displaying posters.
- 9.6. Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.
- 9.7. The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country.

- 9.8. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.
- 9.9. The DSL will check the factual basis of harmful online challenges or hoaxes against a known, reliable and trustworthy source, e.g. the UK Safer Internet Centre, and will carefully consider if a challenge or story is a hoax or is harmful prior to providing any direct warnings to pupils or parents.
- 9.10. The school understands that discussing or naming a specific online hoax can, in some cases, needlessly increase pupils' exposure to distressing content, and will avoid showing pupils distressing content where doing so is not considered absolutely necessary for preventing its spread or easing fears amongst the school community.
- 9.11. Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.
- 9.12. The DSL and head teacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.
- 9.13. Prior to deciding how to respond to a harmful online challenge or hoax, the DSL will decide whether each proposed response is:
 - Factual and avoids needlessly scaring or distressing pupils.
 - Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils that is almost exclusively being shared amongst older pupils.
 - Proportional to the actual or perceived risk.
 - Helpful to the pupils who are, or are perceived to be, at risk.
 - Age-appropriate and appropriate for the relevant pupils' developmental stage.

10. Educating Parents

- 10.1. The school works in partnership with parents to ensure pupils stay safe online at school and at home.
- 10.2. Parents are provided with information about the school's approach to online safety and their role in protecting their children.
- 10.3. Parents are sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.
- 10.4. Parents will be made aware of the various ways in which their children may be at risk online. These risks include, but are not limited to:

- Child sexual abuse, including grooming.
 - Exposure to radicalising content.
 - Sharing of indecent imagery of pupils, e.g. sexting.
 - Cyberbullying
 - Exposure to age-inappropriate content, e.g. pornography.
 - Exposure to harmful content, e.g. content that encourages self-destructive behaviour.
 -
- 10.5. Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.
- 10.6. Parental awareness regarding how they can support their children to be safe online is raised in the following ways:
- Parents' evenings
 - Newsletters
 - Online resources

Useful Resources for Teachers and Parents

Resource	Website
Child Exploitation and Online Protection Centre	www.ceop.gov.uk/
Childnet	www.childnet-int.org/
Digizen	www.digizen.org/
Kidsmart	www.kidsmart.org.uk/
Think U Know	www.thinkuknow.co.uk/
Family Online Safety Institute	http://www.fosi.org
Internet Watch Foundation	www.iwf.org.uk
Internet Safety Zone	www.internetsafetyzone.com
Vodafone digital parenting	www.vodafone.com/content/digital-parenting.html
NSPCC - Share Aware	www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware
Parent Zone	www.theparentzone.co.uk/school

St Peter's Catholic Primary School



Staff, Governor and Visitor Acceptable Use Agreement

ICT and the related technologies, such as email, the internet and mobile devices, are an expected part of daily working life in school. This policy is to help ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All staff are expected to sign this agreement confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with the headteacher.

- I will only use the school's email, internet, learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the headteacher or governing board.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my personal details, such as mobile phone number or personal email address, to pupils.
- I will only use the approved email system for any communications with pupils, parents and other school-related activities.
- I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of the school or accessed remotely when authorised by the headteacher or governing board and with appropriate levels of security in place.
- I will not install any hardware or software on school equipment without the permission of the headteacher.
- I will report any accidental access to inappropriate materials immediately to my line manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with data protection policy and with written consent of the parent or staff member. Images will not be distributed outside the school network without the permission of the parent, member of staff or headteacher in line with data security policy.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).
- I will support and promote the school's Online safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school.

Signature _____

Date _____

Full name _____ (Printed

Acceptable Use Agreement: Pupils

Class: _____

Year: _____

Pupil Acceptable Use Agreement

- I will only use ICT in school for school purposes.
- I will only use my own school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords for the learning platform, school network or for other learning websites.
- I will only open/delete my own files.
- I will make sure that all ICT related contact with other children and adults is appropriate and polite.
- I will not deliberately look for, save or send anything that could offend others.
- If I accidentally find anything inappropriate on the internet I will tell my teacher immediately.
- I will not give out my personal details such as my name, phone number, home address or school.
- I will be responsible for my behaviour when using ICT in school or at home because I know that these rules are to keep me safe.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I know that my use of ICT can be checked and that my parent contacted if a member of school staff is concerned about my safety.
- I will not bring a mobile phone or other personal ICT device into school.

Signature pupil: _____

Signature parent: _____

Date: _____



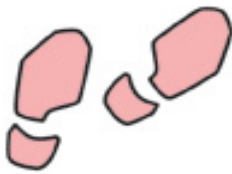
Think then Click



These rules help us to stay safe on the internet

Online safety rules for EYFS and KS1

- ✓ We only use the internet when an adult is with us.
- ✓ We can click on the buttons or links when we know what they do or where they take us.
- ✓ We can use the internet to search for things when an adult is with us.
- ✓ We always stop and ask for help if we get lost on the internet.
- ✓ We can send and open emails with a grown-up.
- ✓ We can write polite and friendly emails to people we know.
- ✓ We never share our names or addresses on the internet.
- ✓ We know that friends are people we know in the real world not people we meet online.





Think then Click



These rules help us to stay safe on the internet

Online safety rules for KS2

- ✓ We ask permission before using the internet.
- ✓ We only look at websites an adult has given us permission to use.
- ✓ We always tell an adult if we have seen, heard or read anything on the internet that has made us feel threatened, uncomfortable or worried.
- ✓ We immediately close a web page if we are unsure.
- ✓ We only send polite and friendly emails to people we know or that an adult has approved.
- ✓ We never give out personal information or passwords.
- ✓ We never arrange to meet anyone we don't know.
- ✓ We do not open emails sent by anyone we don't know.
- ✓ We do not use internet chat rooms.
- ✓ We know that friends are people we know in the real world not people we meet online.

