Developing and Reviewing this Policy

This online safety Policy has been written as part of a consultation process involving the following people:

The Headteacher, Computing Subject Leader, School Admin Support Officer

It has been approved by Governors and will be monitored and reviewed as listed below:

Policy updated - April 2026
Review Date – April 2027

The implementation of this policy will be monitored by **Ben Chaffe, Sally Glennon**

This policy will be reviewed as appropriate by **Ben Chaffe**

Approved by Ben Chaffe (Headteacher) Date 25.4.2026

Approved by Anna Shone (Governor) Date 13/5/2026

VISION AND BELIEF DECLARATION

One family, belonging, believing and learning together

Caton St Paul's C of E Primary School exists to encourage every child to achieve his or her full potential. A caring Christian environment is provided in which children are offered educational opportunities of the highest quality and where all contributions are valued.

The school is distinguished by the quality of care its members extend to each other and the wider community and by the fostering of spiritual development, mutual love, respect and responsibility.

We aim to provide a rich, varied and stimulating learning environment that allows all children to develop their skills and abilities to their full potential.

Online Safety Policy 2025 Caton St. Paul's Primary School

1. Introduction

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact. Our Online Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings.

This policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

2. Caton St. Paul's Vision for Online Safety

Our school strives to provide a diverse, balanced and relevant approach to the use of technology, where children are encouraged to maximise the benefits and opportunities that technology has to offer. Our aim is that everyone at Caton St Paul's is equipped with the knowledge and skills to safeguard themselves online. This will include:

- Learning about the safe use of new technologies.
- Recognising and managing potential risks associated with our online world.
- Behaving responsibly online.

3. The role of the school's Online Safety Champion

Our Online Safety Champion is Mr. Ben Chaffe.

The roles of the Online Safety Champion are as follows:

- Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including online safety agreements. This will be overseen by the Online Safety Champion, Mr. Ben Chaffe.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an online safety incident occur.
- Ensure the Online Safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with online safety issues and guidance through liaison with the Local Authority Schools' ICT team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging online safety advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, SLT, staff, pupils and governors are updated as necessary.

- Liaising closely with the school's Designed Senior Person / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

4. Policies and practices

This section of the Online Safety Policy sets out the school's approach to online safety along with the various procedures to be followed in the event of an incident. This online safety policy should be read in conjunction with the following documentation:

- Staff and Governors online safety agreement.
- Parent online safety agreement.
- Pupil online safety agreement.
- ICT Security Framework policy
- Behaviour Policy
- Whistle blowing policy

4.1 Security and data management

In line with the requirements of the General Data Protection Regulation (2018), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary (see privacy notice)
- Only transferred to others with adequate protection.
- All laptops are password protected.
- All children have class or individual passwords and are encouraged not to share it.

All data in the school is kept secure and staff are informed of what they can or cannot do with data through the Online Safety Policy and statements in the online safety agreements.

- The school maps key information that is held.
- There is a named person, Mr. Ian Gittins with responsibility for managing information.
- Relevant staff know the location of data.
- All staff with access to personal data understand their legal responsibilities.

- The school ensures that data is appropriately managed, both within and outside the school environment, through the use of secure emails.
- Staff are aware that they should only use approved means to access, store and dispose of confidential data. Pupil data is kept for 25 years and safely disposed of by the school's Data Protection Officer.
- Personal devices, e.g. Smartphone, iPads may not be used to access data on the school system.
- Risk of data loss is minimised by having daily back up of the administration networks (SIMS) and daily back up for the curriculum network.

4.2 Use of mobile devices

The use of mobile devices offers a range of opportunities to extend children's learning. Staff are aware that some mobile devices e.g. mobile phones, game consoles or net books can access unfiltered internet content. These devices are not to be used by pupils in school. Pupils are urged not to bring mobile phones into school. If a phone is brought in by mistake or for the child's journey to and from school then pupils are asked to hand in the phone to the school office on entry to school for safe keeping until the end of the day. Pupils then have no access to their phones during the school day and will be handed the phone back by the class teacher as they leave the school building.

4.3 Use of digital media

Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites.

It is the responsibility of the online safety champion to ensure all users are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media.

- At school photographs and video of pupils and staff are regarded as personal data in terms of The Data Protection Act (2018), and at school we seek written permission for their use from individuals and pupils' parents or carers.
- The school seeks consent from the pupils' parent/carer or member of staff who appears in the media or whose name is used.
- The parental/carer permission is obtained at the beginning of the academic year and is updated on a yearly basis. However, parents have a right to change this during the academic year if deemed necessary.
- The school will not re-use any photographs or videos after staff and pupils have left the school without further consent being sought.
- Parents/carers, who have been invited to attend school events, are allowed to take videos and photographs. We ask the parents not to share these images on Social Network sites.
- All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites. It is forbidden for staff to post images or video of pupils taken at school, in any school activities, on any personal Social Network sites.
- The school ensures that photographs/videos are only taken using school equipment and only for school purposes e.g. website, brochure or display.
- The school ensures that any photographs/videos are only accessible to the appropriate staff/pupils.
- Staff are not allowed to store digital content on personal equipment. Staff are not to use their own

cameras without prior permission from the Headteacher.

- When taking photographs/video, staff ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted.
- Staff, parents/carers and pupils are made aware of the dangers of publishing images and videos of pupils or adults on Social Network sites or websites without consent of the persons involved.
- All staff digital communications with learners, parents and carers and others should be on a professional level and only carried out using official school systems and devices (where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements).
- All users are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.
- The guidelines for safe practice relating to the use of digital media, as outlined in the school's policy are monitored by the online safety Champion, S.L.T and Governors on an annual basis.

4.4 Communication technologies

At Caton St. Paul's we use a variety of communication technologies and are aware of the benefits and associated risks.

Email

- All users have access to Microsoft 365 as the preferred school email system.
- Only official email addresses are used between staff and with pupils/parents when personal and sensitive data is involved.
- Unless necessary, all official emails should not be dealt with using personal equipment e.g. smart phones, iPads etc... All teaching staff are provided with a school laptop to access their email account out of hours.
- The Lancashire Grid for Learning filtering service reduces the amount of SPAM (Junk Mail) received on school email accounts.
- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
- All users are aware that email is covered by The Data Protection Act (2018) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users are aware that all email communications may be monitored at any time in accordance with the online safety agreement.
- Anything being sent by pupils must be authorised by a member of staff.
- All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- Our school will include a standard disclaimer at the bottom of all outgoing emails (see below).
- Children are able to email using Purple Mash: this only allows them to email each other, or staff members and no-one external to the organization. Google Classroom online system may be used to teach children

how to safely use email. This facility will be disabled between lessons.

Example school e-mail disclaimer:

This e-mail and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent Caton St. Paul's C of E Primary School. If you are not the intended recipient, you must not use, disseminate, forward, print or copy this e-mail or its contents. If you have received this e-mail in error, please contact the sender. Please note that e-mail may be monitored in accordance with both school policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.

Social networks

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Twitter, Tik Tok and Instagram. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a blog or comments published by the user. As a user on a Social Network site, you may have access to view other user' content, send messages and leave comments. NB: Many Social Network sites have age restrictions for membership e.g. Facebook minimum age is 13 years old.

All staff are advised that:

- They must not give personal contact details to pupils. Caution should be used when giving personal contact details to parents including mobile phone telephone numbers, details of any blogs or personal websites.
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- If a social network site is used, details must not be shared with pupils and privacy settings be set at maximum.
- Pupils must not be added as friends on any Social Network site.
- Adults are aware of the age restrictions for Social Networking sites and have a duty of care to report any known user that is under the minimum age to the Online Safety Champion.

Remember: whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Mobile phones

- Mobile phones may be used by staff and visitors at appropriate times and only to be used in the staffroom during school hours. Staff and visitors are allowed to use mobile phones in classrooms, when pupils are not present. It is expected that staff and visitors turn their mobile phones on silent during curriculum time. However, in exceptional circumstances prior arrangements can be made with the Headteacher. Mobile phones must not be left in a place where they can be easily seen or accessed by pupils at any point.
- School has a designated mobile phone for use for school activities e.g. After School Club.

- It is acceptable to use personal mobile phones for school activities or in an emergency by prior arrangement by the Headteacher.
- It is not acceptable to use personal mobile phones to support lessons without prior arrangements from the Headteacher.

Websites and other online publication
(Including podcasts, videos, 'Making the News' and blogs)

A school website and other online publications e.g. podcasts or blogs, provide an effective way to communicate information. The following statements are what our school deems acceptable and unacceptable use of web sites and other online publication:

- Staff or pupil personal contact information will not be published. The contact details given online will be the school office.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The nominated governor has editorial responsibilities and is responsible for ensuring that content is accurate and appropriate.
- Procedure outlined in section 4.3 (Use of digital media) of this policy will be implemented in the publication of pupil's images, video and work on the school website.
- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Group photographs will be used in preference to full-face photos of individual children.
- Pupils full names will not be used anywhere on the school website 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.
- Named work can only be published with the permission of the pupil and parents/carers.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
- The school website and school platforms will be used to communicate online safety messages to parents/carers, to provide guidance on the use of digital media.
- Staff and governors are aware what information is appropriate to publish and what information is not appropriate to publish on the school's website.
- The school's website may be edited by school staff who have permission from the Head Teacher. Pupils may not edit the website.
- Staff and governors are aware that they may not publish content which is subject to copyright / personal intellectual copyright restrictions.
- A nominated governor will be responsible for checking the content on the school website annually.
- Downloadable materials will be in read-only format (e.g. PDF) to prevent content being manipulated and potentially re-distributed without the school's consent.

Video conferencing

- Parents will be asked for permission before pupils take part in video conferencing sessions.
- Approval by the Headteacher must be obtained in advance of the video conference taking place. All sessions will be logged including the date, time and the name of the external organisation/person(s) taking part.
- Pupils using video conferencing equipment should be supervised at all times.
- All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to 'hang up' the call.
- Staff understands that copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.
- Video conferencing will be used to keep in contact with children in the event of prolonged periods of remote education. Staff, children and parents will be made aware of the expectations for ensuring online video conferencing is safe and successful.

Others

The School will adapt/update the online safety policy in light of emerging new technologies and any issues or risks associated with these technologies.

4.5 Acceptable Use Policy (AUP)

At Caton St. Paul's the Acceptable Use Policy (AUP) is known as the online safety agreement.

Our online safety agreement is intended to ensure that all users of technology within school will be responsible and stay safe. It ensures that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

Online safety agreements (Appendix 1,2,3) are used for staff, governors, visitors, supply teachers and pupils and must be signed and adhered to by users before access to technology is allowed. This agreement is as a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology is kept in school. It is the responsibility of the Online Safety Champion to make this information available to all staff.

Our school online safety agreements aim to:

- Be understood by each individual user and relevant to their setting and purpose.
- Be regularly reviewed and updated.
- Be regularly communicated to all users, particularly when changes are made to the online safety Policy/online safety agreements.
- Outline acceptable and unacceptable behaviour when using technologies, for example:
    - o cyberbullying
    - o inappropriate use of email, communication technologies and Social Network sites and any online content
    - o acceptable behaviour when using school equipment /accessing the school network.
- Outline the ways in which users are protected when using technologies e.g. passwords, virus

protection and filtering.

- Provide advice for users on how to report any failings in technical safeguards.
- Clearly define how monitoring of network activity and online communications will take place and how this will be enforced.
- Outline sanctions for unacceptable use and make all users aware of the sanctions (linked to our Behaviour Policy).
- Stress the importance of online safety education and its practical implementation.
- Highlight the importance of parents/carers reading and discussing the content of the online safety agreement with their child.

4.6 Dealing with incidents

At Caton St Paul's an incident log is completed to record and monitor offences. All incidents must be reported to the Online Safety Champion. This is audited on a regular basis by the online safety champion and Headteacher.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). ***Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.*** It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident.

Potential illegal content must always be reported to the Internet Watch Foundation (http://www.iwf.org.uk). Examples of illegal offences are:

1. Accessing child sexual abuse images
2. Accessing non-photographic child sexual abuse images
3. Accessing criminally obscene adult content
4. Incitement to racial hatred

More details regarding these categories can be found on the IWF website; http://www.iwf.org.uk

Inappropriate use

It is more likely that at school we will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and proportionate to the offence. The school will decide what constitutes inappropriate use and the sanctions to be applied. Some examples of inappropriate incidents are listed below with suggested sanctions.

Incident	Procedure and sanctions
Accidental access to inappropriate materials.	• Minimise the webpage / turn the monitor off / • Tell a trusted adult. • Staff enter the details into the incident log and report to LGFL filtering services if necessary. • Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	• Inform online safety champion. • Enter the details in the incident log. • Additional awareness raising of online safety issues and the online safety agreement with individual pupil / class. • More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. • Consider parent / carer involvement.
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chat and forums in an inappropriate way.	

- Online safety incidents will be reported to the online safety champion who will record the incidents into the Online Safety Incident Log (electronically). The Online Safety Champion will report all incidents to the Headteacher to discuss appropriate actions to be taken.
- All staff are aware of the different types of online safety incidents and how to respond appropriately.
- All pupils are informed of procedures through discussions from members of staff.
- Incidents are monitored by the Online Safety Champion and Headteacher on a regular basis.
- The Headteacher will decide on which point that parents or carers are informed.
- These procedures are in place to protect staff and escalate a suspected incident / allegation involving a staff member.

5. Infrastructure and technology

At Caton St. Paul's Primary School we ensure that the infrastructure/network is as safe and secure as possible. We subscribe to the B4RN Broadband Service and our filtering is provided by the Lightspeed filtering service. It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. As a school, we have a Sophos Anti-Virus subscription (through Lancashire educational and digital services), which is installed on computers in school and then configured to receive regular updates.

We offer the following guidance regarding security:

Pupil access

- All pupils are supervised by staff when accessing school equipment and online materials

Passwords

- All staff are aware of the guidelines from the National Cyber Security Centre in relation to passwords https://www.ncsc.gov.uk/training/v4/Top+tips/Web+package/content/index.html#.

- All users of the school network have a secure username and password.
- All users of the school Microsoft 365 Tennant will use 2 factor authentication wherever possible.
- All pupils have an individual user name and password to login to the Chromebooks.
- The administrator password for the school network is available to the Headteacher and is kept in a secure place.
- Staff and pupils are reminded of the importance of keeping passwords secure.
- All users of the school network are reminded to change their passwords on a regular basis.

Software/hardware

- The school has legal ownership of all software.
- The school has an up-to-date record of appropriate licenses for all software and the ICT Subject Leader is responsible for maintaining this.

Managing the network and technical support

- Servers, wireless systems and cabling are securely located and physical access restricted.
- The security of the school network is maintained by the ICT Technician.
- The safety and security of the school network is reviewed annually.
- Computers are regularly updated with software updates/patches as required.
- Staff and pupils have clearly defined access rights to the school's network. Guests such as student teachers will have the same restricted access rights as the pupils. There is a separate server and secure logins for the school administration computers.
- Staff and pupils are required to log out of a school system when a computer/digital device is left unattended.
- Users should report any suspicion or evidence of a breach of security to the Online Safety Champion or the Headteacher. This is recorded on the online safety monitoring form, to be monitored by the Headteacher.
- Removable storage devices may not be used in school, unless authorised by the Online Safety Champion or Head Teacher.
- School equipment including teacher laptops must not be used for personal and family use.
- Personal equipment e.g. iPads, Smartphones, net books etc... must not be used for storing, opening and working on sensitive school data, including images and video of children.
- Staff are made aware that network monitoring/remote access may take place and this is in accordance with the Data Protection Act 2018.
- External technical support providers (e.g. the ICT Technician) are made aware of the school's Online Safety Policy.
- The technical support staff are managed overall by the Headteacher and on a week to week basis by the Computing Subject Leader.

Filtering and virus protection

- Filtering is provided by the Lightspeed filtering service.
- Filtering is managed by the ICT Technician /Computing Subject Leader. Monthly checks of the filtering system are carried out by the Computing subject leader/ICT Technician, and monitored by the Headteacher.

- Virus protection (Sophos) is provided through Lancashire educational and digital services and regularly updated.
- Staff must apply to the Headteacher for blocking and unblocking specific websites.
- Staff must report suspected or actual computer virus infection to both the ICT Subject Leader and the ICT Technician.
- School laptops used at home are set to regularly update virus protection software.

6. Education and training

In 21st Century society, staff and pupils need to be digitally literate and aware of the benefits technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.

The main areas of online safety risk that our school needs to be aware of and consider (as suggested in The DfE Keeping Children Safe in Education) are:

Area of risk	Example of risk
Commerce: Pupils need to be taught to identify potential risks when using commercial sites.	Advertising e.g. SPAM Privacy of information (data protection, identify fraud, scams)
Content: Pupils need to be taught that not all content is appropriate or from a reliable source.	Illegal materials Inaccurate/bias materials Inappropriate materials Copyright and plagiarism User-generated content e.g. YouTube, Flickr, cyber-tattoo, sexting.
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	Grooming Cyberbullying Contacting Inappropriate emails / instant messaging/blogging. Encouraging inappropriate contact.
Conduct: Pupils need to be taught that some online behaviour increases the likelihood of, or causes harm.	Making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography) Sharing other explicit images Online bullying

6.1 Online safety across the curriculum

It is vital that pupils are taught how to take a responsible approach to their own online safety. Caton St. Paul's provides suitable online safety education to all pupils. This is ensured through:

- Regular, planned online safety teaching within a range of curriculum areas. Online safety is in aspect of all computing curriculum plans.
- Online-Safety education is adapted for pupils with special educational needs.
- Pupils are made aware of the impact of Cyberbullying and how to seek help if they are affected by these issues, e.g. using peer mentoring.
- Pupils are taught to critically evaluate materials and develop good research skills through cross-curricular teaching and discussions.
- The school ensures that pupils develop an understanding of the importance of the online safety agreements and are encouraged to adopt safe and responsible use of ICT both within and outside school.
- Pupils are reminded of safe Internet use e.g. classroom displays, online safety rules (See Appendices).

Caton St Paul's recognises that misinformation, disinformation (including fake news), and conspiracy theories are identified within Keeping Children Safe in Education (KCSIE) 2025 as online content risks that may harm pupils' wellbeing and safety.

- Misinformation refers to false or misleading information shared without intent to deceive.
- Disinformation is false information deliberately created and shared to mislead
- Conspiracy theories are unverified or false explanations of events, often involving perceived hidden plots or agendas.

The school will address these risks through a whole-school safeguarding approach by teaching pupils, in an age-appropriate way, to develop critical thinking and digital literacy, enabling them to evaluate online sources, recognise bias and manipulation, and understand the potential impact of misleading content on health, relationships and decision-making. We will ensure that filtering and monitoring systems help reduce exposure to harmful content, and that staff are trained to identify and respond to concerns, reporting to the Designated Safeguarding Lead where pupils may be vulnerable to harmful or extremist narratives or are experiencing distress. We will work in partnership with parents and carers to promote safe and informed use of technology and will review this provision regularly in line with emerging risks and statutory guidance.

6.2 Online safety – Raising staff awareness

- The Online Safety Champion will provide advice / guidance to all members of staff to ensure they are regularly updated on their responsibilities as outlined in this policy.
- The Online Safety Champion will provide advice/guidance or training to individuals as and when required.
- Online safety training ensures staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.
- All staff are expected to promote and model responsible use of ICT and digital resources.
- Online safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's Online Safety Policy and online safety agreements.
- Regular updates on Online Safety Policy, online safety agreements, curriculum resources and general

online safety issues are discussed in staff / TA meetings.

6.3 online safety – Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008).

Our school offers regular opportunities for parents/carers and the wider community to be informed about online safety, including the benefits and risks of using various technologies. For example, through the school's website, bespoke parents online safety awareness workshops, promotion of external online safety resources/online materials and the school Facebook page. An online safety article is included in the school newsletter every half-term.

6.4 Online safety – Raising Governors' awareness

Our school considers how Governors, particularly those with specific responsibilities for online safety, ICT or child protection, are kept up to date. This is through discussion at Governor Meetings, attendance at Local Authority Training, CEOP or internal staff/parent meetings.

The Online Safety Policy will be approved by the governing body and made available on the school's website. There is a Governor responsible for online safety who will meet with our online safety champion on a regular basis.

7. Standards

- The effectiveness of the online safety policy will be monitored through planning scrutiny, lesson observations, formal conversations with staff and pupils, and monitoring of website access, downloading and email accounts.
- Online safety incidents will be monitored and recorded by the Online Safety Champion.
- The introduction of new technologies will be risk assessed and these assessments included in the online safety policy.
- Any recurring incident will be analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children.
- Monitoring of online safety incidents will contribute to changes in policy and practice as necessary. Any changes to policy and practice will be reported to staff and governors through meetings, to pupils by their teacher and to parents via the school newsletter / website.
- Online safety agreements will be annually reviewed and include reference to current trends and new technologies.

This policy was written by Mr. Ben Chaffe. This policy was reviewed and adapted by Mr. Ben Chaffe and approved at the full governors meeting in _____.

List of Appendices

Appendix 1 .....online safety agreement: Parents
Appendix 2 .....online safety agreement: Pupils
Appendix 3 .....online safety agreement: Staff and Governors
Appendix 4 .....EYFS & KS1 Rules of responsible use.
Appendix 5 .....KS2 Rules for responsible use

Appendix 1: online safety agreement: parents

Parent / guardian name: _____

Pupil name: _____

Pupil class: _____

Parent's consent for Internet access

As the parent or legal guardian of the above pupil, I grant permission for my child to have access to use the Internet, e-mail and other ICT facilities at school. I know that my child has signed an online safety agreement form and that they have a copy of the 'rules for responsible use'.

I understand that the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies. However, I recognise that all staff at Caton St Paul's will take every responsible precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricting access to email, employing appropriate teaching practice and teaching online safety skills to pupils.

Signature: _____ **Date:** _____

Parent's consent for use of images

We regularly take photographs/videos of children at our school. These may be used in our school prospectus, in other printed publications, on our school website, on school displays or on our school Facebook page. Occasionally, our school may be visited by the media who will take photographs/videos of an event or to celebrate a particular achievement. These may then appear in local or national newspapers, websites or on televised news programmes. In order that we can protect your child's interests, and to comply with the Data Protection Act (2018), please read the Conditions of Use on the back of this form, then answer questions 1-5 below.

Please sign, date and return the completed form (one for each child) to school as soon as possible**.**
(Please Circle)

1) May we use your child's photograph in printed school publications? Yes / No
2) May we use your child's photograph for school display purposes? Yes/No
3) May we use your child's image on our school website? Yes / No
4) May we use your child's image on our school Facebook page? Yes/No
5) May we video your child during appropriate teaching and learning and performing activities / events? Yes / No
6) May we allow your child to appear in the media as part of school's involvement in an event? Yes / No

I have read and understand the conditions of use attached to this form

Signature: _____ **Date:** _____

Conditions of Use

1. This form is valid for the time that your child is a pupil at Caton St Paul's C.E. Primary School.

2. The school will not re-use any photographs or videos after your child leaves this school without further consent being sought.

3. The school will not use the personal contact details or full names (which means first name and surname) of any pupil or adult in a photographic image, or video, on our website/Facebook) or in any of our printed publications.

4. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article without prior permission.

5. We will only use images of pupils who are suitably dressed.

6. Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.

Notes on use of images by the media

If you give permission for your child's image to be used by the media then you should be aware that:

1. The media will want to use any images/video that they take alongside the relevant story.

2. It is likely that they will wish to publish the child's full name, age and the school's name in the caption for the picture (possible exceptions to this are large group or team photographs)

3. It is possible that the newspaper will re-publish the story on their website or distribute it more widely to other newspapers or media organisations (including social media).

Appendix 2: Online safety agreement:

Pupils Rules for responsible use

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. It is important that parents/carers read and discuss the following statements with their child, understanding and agreeing to follow the school rules on using ICT, including the internet.

Key stage 1 online safety rules for responsible use

These rules help us stay safe on the internet:

- 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.
- We can search the Internet with an adult.
- We always ask if we get lost on the Internet.
- We can send and open e-mails together.
- We can write polite and friendly e-mails to people that we know.
- We ask permission before using the school computers.
- We ask permission before using the printer.

Key Stage 2 online safety rules for responsible use

- We will ask permission before using the school's computers and equipment.
- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately minimise any webpage we are not sure about.
- We only e-mail people an adult has approved.
- We will only send polite and friendly e-mails.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.
- We will ask permission before using our own pen drives.
- We ask permission before using the printer.

Parent/ Carer Signature

We have discussed this online safety agreement and..... [Print child's name] agrees to follow the online safety rules for responsible use and to support the safe use of ICT at *Caton St Paul's C of E Primary School.*

Pupil signature.....

Parent /Carer Name (Print) ……

Parent /Carer (Signature) ……

Class …… Date……

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

Appendix 3: online safety agreement: Staff, Governors and Volunteers

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

2. I will be an active participant in online safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.

3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.

4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.

5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.

6. I will respect copyright and intellectual property rights.

7. I will ensure that all electronic communications with pupils and other adults are appropriate.

8. I will not use the school system(s) for personal use during working hours.

9. I will not use personal equipment e.g. laptops, smart phones, iPads etc... to access sensitive school data.

10. I will not install any hardware or software without the prior permission of Mr. Ian Gittins.

11. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.

12. I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.

13. I will report any known misuses of technology, including the unacceptable behaviours of others.

14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.

15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.

16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other user' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

17. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.

19. I will take responsibility for reading and upholding the standards laid out in this agreement. 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.

20. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……

Date ……

Full Name .....(PRINT)

Position/Role.....

Please circle

1) May we use your photograph in printed school publications? Yes / No
2) May we use your photograph for school display purposes? Yes/No
3) May we use your image on our school website? Yes / No
4) May we use your image on our school Facebook page? Yes/No
5) May we use your image in external media? Yes / No

Appendix 4: EYFS & KS1 Rules for responsible use

These Key stage 1 rules help us stay safe on the internet

Think then Click

 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.

 We can search the Internet with an adult.

 We always ask if we get lost on the internet.

 We can send and open e-mails together.

 We can write polite and friendly e-mails to people that we know.



We ask permission before using the school computers.



We ask permission before using the printer.

Appendix 5: KS2 Rules for responsible use

These Key stage 2 rules help us stay safe on the internet

Think then Click

- We will ask permission before using the school's computers and equipment.
- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately minimise any webpage we are not sure about.
- We only e-mail people an adult has approved.
- We will only send polite and friendly e-mails.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.
- We will ask permission before using our own pen drives.

- We ask permission before using the printer.



