ST.ANNE'S COPP CHURCH OF ENGLAND PRIMARY SCHOOL, GREAT ECCLESTON

ONLINE SAFETY POLICY



"Let us love, not in word, but in truth and action." (1 John 3:18)

SEPTEMBER 2026

Approved by GB: Sarah Hall
Next review due: September 2027

In building solid foundations for every unique individual and putting God's love at the centre of all we do, our children learn to embrace our diverse world. We encourage our children to learn universally in order to understand our heritage and roots as a village, town, region and nation. Through strong community links, our children grow in compassion and understanding, promote justice and possess commitment and aspire to make a positive difference. We offer an ambitious curriculum that ignites curiosity along with high personal expectations that fosters resilience and which enables them to flourish. Our children are easily distinguished by the courage they show when making brave choices and understand the importance of becoming the very best versions of themselves.

Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

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.

Security and data management

Data is kept securely at St.Anne's Copp Church of England Primary School, Great Eccleston and all staff are informed as to what they can/cannot do with regard to data.

- All staff computer areas are password protected
- Staff use memory sticks; these are password protected and are kept in a secure place at all times
- Paper-based documents must be shredded
- Data must not be passed on to individuals outside of school unless parents have given permission
- Our school staff have had GPDR training and we follow GPDR protocol within school

Use of mobile devices

We recognise the use of mobile devices offers a range of opportunities to extend children's learning and for their safety; however in line with our Safeguarding Policy and Mobile Phone Policy, staff and visitors must have their phones switched off at all times during the school day and when children are present. There may be limited circumstances in which staff are required or authorised to use a mobile phone or similar device for a legitimate professional purpose. This may include an urgent or exceptional situation, safeguarding or emergency communication, or an approved school-related function. Such use must be proportionate, necessary and in accordance with the school's safeguarding, data protection and acceptable-use requirements.

- Mobile phones are not permitted to be used by pupils during the school day. This includes lessons, movement between lessons, breaktimes, lunchtimes and all other periods of the school day. The school will maintain a mobile-phone-free environment in accordance with Department for Education statutory guidance effective from 1 September 2026.
- Pupils in Years 5 and 6 who need to bring a mobile phone to school must hand it directly to a member of class staff on arrival. The phone will be stored securely in the school's designated secure storage facility and will be returned to the pupil at the end of the school day.
- Pupils in Reception to Year 4 must not bring a mobile phone or other mobile communication device to school, unless there are exceptional circumstances which have been discussed with and agreed in

advance by the Headteacher. Any agreed exception will be subject to the same requirements regarding secure storage and non-use during the school day.

Please also see our Mobile Phone Policy

Use of digital media

Children and staff are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below. Parents are asked to give consent for their child to be videoed/photographed when their child starts at St.Anne's Copp Church of England Primary School, Great Eccleston. All staff are made aware of which children can be photographed/videoed and whether or not their pictures can be used on the website, in the newspaper etc. Staff delete photographs weekly from Teacher iPads. Some photos may be stored on the school network for curriculum evidence purposes, which is secure.

Use of AI

Artificial Intelligence (AI) may be used at St. Anne's Copp CE Primary School, Great Eccleston only when it demonstrably supports teaching, learning or administration while upholding pupil safety, privacy and equality. Staff must supervise all AI tools, ensuring they are age appropriate, free from harmful content and do not require pupils to share personal data beyond first names. AI must complement—not replace—professional judgement; any AI generated output used for assessment, feedback or communication must be checked for accuracy, bias and suitability before sharing with pupils or parents. No pupil accounts may be created on external platforms without written parental consent and a data protection impact assessment. The school will log and review AI use termly, provide staff training, and disable or remove any tool that contravenes safeguarding, UK GDPR or our Acceptable Use and Online Safety policies.

Misinformation, Disinformation and Conspiracy Theories

The school recognises that children may encounter misinformation, disinformation and conspiracy theories when using the internet, social media or other digital platforms. Staff will support pupils in developing critical thinking and digital literacy skills so they can question, verify and evaluate online content. These skills are apportioned directly within our half termly online safety sessions in school. Where misleading or harmful information is identified, staff will address it in an age-appropriate manner, helping pupils understand the importance of reliable sources and respectful discussion. The school will also work with parents and carers where necessary to promote safe and responsible engagement with online information.

Communication technologies

Email: All staff have a school email address, which is part of the Lancashire Grid for Learning Service on Office Portal 365. Only official email addresses will be used to contact staff/parents.

The Lancashire Grid for Learning filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of SPAM should be marked as junk and reported to the Westfield Centre. Staff in school adhere to guidance on monitoring and filtering in line with Keeping Children Safe in Education 2026.

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 (1988) 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 Acceptable Use Policy.

All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Social Networks: (See also Social Networking Policy)
As a school we make it clear to pupils and parents that social networking sites are not appropriate for primary aged children.

Staff who use social networking sites outside of school are reminded regularly about school confidentiality.

Social Network sites allow users to be part of a virtual community. Current popular examples of these are Facebook, Twitter, Instagram and TikTok. These sites provide users with simple tools to create a profile or page including basic information about the user, photographs, and possibly a Page 4 blog or comments published by the user. As a user on a Social Network site, you may have access to view other users' 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 need to be aware of the following points:
- They must not give personal contact details to pupils or parents/carers including mobile 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 and ex pupils must not be added as "friends" on any Social Network site.
- 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.

Online Hoaxes and Harmful Online Challenges
A hoax is a deliberate lie trying to appear truthful and harmful online challenges generally involve users recording themselves taking a challenge and then sending the video through social media channels.

- Parents should be aware of what their child is accessing.
- School to build into Online Safety lessons about appropriate phone usage.
- Additional half-termly Online Safety lessons are taught across school each year.
- School to provide a safe and open space for pupils to ask questions and share concerns about what they experience online without being made to feel foolish or blamed. (KCSIE 2026)
- Pupils to report any concerns and feel confident they will be taken seriously.

Websites and other online publications
The school website is updated by staff at St.Anne's Copp Church of England Primary School, Great Eccleston and maintained by a third party. It is used to communicate information with current parents and prospective parents. Website information is overseen by the Computing Subject Leader and Headteacher.

Interactive Sites:
The school uses safe interactive sites such as Spelling Shed and TTRocks as an aid to learning. Such sites are monitored by a designated member of staff to ensure that they are school based.

Acceptable Use Policy (AUP)
There is an Acceptable Use Policy in place for all users (see separate policy at the back of this policy).

Dealing with incidents
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) www.iwf.org.uk .There should be NO personal investigation, interference or sharing of evidence as this may mean that an illegal offence has been committed.
Examples of illegal offences are:
- accessing child sexual abuse images;
- accessing non-photographic child sexual abuse images;
- accessing criminally obscene adult content;
- incitement to racial hatred;

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

Inappropriate use
Examples of inappropriate use include:

Usage	Action
Accidental access to inappropriate materials.	Minimise the webpage/turn the monitor off. Child tell an adult. Adult report to LGfL if necessary.
Persistent "accidental" offenders (child)	Discussion with pupil. Monitoring of IT use. Disciplinary action if necessary.
Persistent "accidental" offenders (adult) Using other people's logins and passwords maliciously (adult) Bringing inappropriate electronic files from home. Using chats and forums in an inappropriate way.	Online safety training Revision of APU regulations Disciplinary action
Using other people's logins and passwords maliciously. Deliberate searching for inappropriate materials.	Computing Lead to investigate Enter details into the Behaviour Log. Online safety training for child/class/whole school. Revision of APU regulations

More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy and parents/carers may be involved.

Incidents should be reported to the Computing Lead in the first incidence. These may then be referred to the Headteacher/DSP if child protection is compromised.

The Headteacher receives regular school digital analysis reports. This enables effective and robust internal tracking of websites and searches conducted.

Regular training will take place for staff by the Computing Lead so that all staff are aware what procedures are in place, how they deal with incidents and how these are logged.

Pupil Access:
Children are only allowed to access the internet when they are with a member of St Anne's Copp C of E staff. Children in Key Stage 2 have their own individual log ins.

Passwords:
All staff members who have access to the school network have a secure username and password which they do not share with anyone else.

The administrator password is known by the IT manager, the Headteacher and the IT Technician.

Software/hardware:
When purchasing software we always aim to buy site licences.
The licences are held by the IT manager.
Software is installed by the IT Technician or the IT manager.
Obsolete and out of date equipment and software is disposed of responsibly.

Managing the network and technical support:
The school is hardwired.
There are also wireless points for use with laptops and iPads.
The safety and management of the school network is dealt with by the IT technician.

Filtering and virus protection:
St.Anne's Copp Church of England Primary School, Great Eccleston uses the LGFL filtering service.

Education and Training
Education and training are essential components of effective online safety provision. Equipping individuals, particularly pupils, with the appropriate skills and abilities to recognise the risks and how to deal with them is fundamental. Online safety guidance is embedded within the curriculum and advantage taken of new opportunities to promote online safety.

Governors have safeguarding training, including Online Safety, at induction. The training equips them with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures in place in school are effective and support the delivery of a robust whole school approach to safeguarding. (KCSIE 2026)

Managing Allegations and Safeguarding Concerns
At St. Anne's Copp CE Primary School, safeguarding underpins all aspects of behaviour management - including online safety. Where an allegation or safeguarding concern arises in relation to the online behaviour of children towards one another (child-on-child abuse), the school will follow statutory guidance set out in Keeping Children Safe in Education (KCSIE, Sept 2026) and the school's Safeguarding and Child Protection Policy.

Allegations Relating to Pupils
When concerns are raised about child-on-child online behaviour, the Designated Safeguarding Lead (DSL) will follow the school's Safeguarding Policy and carefully consider:

- The wishes of the victim in terms of how they want to proceed
- The nature of the alleged incident
- The ages of the children involved
- The developmental stages of the children involved
- Any power imbalance between the children
- Whether the incident is a one-off or part of a sustained pattern of abuse
- Any ongoing risks to the victim, other children, or staff

- Wider contextual safeguarding issues

Following a report of sexual violence or harassment, the DSL (or Deputy DSL) will carry out an immediate risk and needs assessment considering:

- The victim
- The alleged perpetrator
- Other children, staff, and the wider school community

Where required, a written risk assessment will be produced, informed by the voice of the children, and shared (on a need-to-know basis) with relevant staff. Parents/carers will be consulted, and assessments will be reviewed at least termly, or sooner if circumstances change.

All decisions will be guided by KCSIE 2026 (Part 5) and in consultation with external agencies where appropriate.

Safety across the curriculum and communication:

- Online safety is mentioned regularly in general lessons and each year group has dedicated safety lessons.
- All children have online safety lessons every half term (6 a year) organised in a progressive and planned way by the Computing Lead.
- Online Safety is embedded within all curriculum planning in all year groups in school.
- Regular online safety updates are passed to staff.
- We also inform our parents about local safety events.
- Reminders are sent home about online safety in newsletters to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems school uses to filter and monitor online use. (KCSIE 2026)
- Regular online safety updates are passed to staff.
- A child friendly online safety policy is shared with all children at the beginning of the year.
- Governors also receive updates on online safety and awareness.

This policy will be reviewed each year and also in the light of new developments in technology and guidance from Lancashire ICT Services and Keeping Children Safe in Education.