



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



# SOCIAL NETWORKING POLICY



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

Approved by GB: April 2025  
Next review due: April 2026

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

**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 CE 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 but these must be 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 GDPR training and we follow GDPR 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 there are no plans at the moment for mobile phones to be used as part of a lesson. When this happens, parents will be informed of the reason why mobiles are to be used in the lesson and the educational merits of such.

- Children in Years 5 and 6 may bring a mobile phone to school but it must be left with the class teacher
  - Staff may use personal mobiles in their breaks, lunchtime or in their own time in a private space
  - Staff mobiles are not used to record learning. Staff use staff iPads and content should be downloaded immediately, where possible, to a relevant computer and deleted from the staff device
- \*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.

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

Parents are asked to give consent for their child to be videoed/photographed when their child starts at St. Anne's Copp CE 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. All photos/videos are stored on the school network which is secure.

### **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.

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:**

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 and Twitter (X). 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 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.

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

- 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.

**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.

Websites and other online publications

The school website is maintained by staff at St. Anne’s Copp CE Primary School , Great Eccleston and is used to communicate information with current parents and prospective parents. Website information is overseen by the Computing subject leader and head teacher.

**Interactive Sites:**

The school uses safe interactive sites such as Times Table Rockstars as an aid to learning. Such sites are monitored by a designated member of staff to ensure that they are school based.

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](http://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.

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

Persistent “accidental” offenders (child)	Discussion with pupil. Monitoring of ICT 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.

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.

#### Infrastructure and technology

As a school we subscribe to the Lancashire Grid for Learning/CLEO Broadband Service and internet content filtering is provided by default. The filtering and monitoring service offers a high level of protection but occasionally unsuitable content may get past the filter service. School alert Westfield immediately if there are any immediate concerns.

Sophos Anti-Virus software is included in the school's subscription, and has been installed on all computers in school and they are configured to receive regular updates. Children and staff are trained in what to do if they come across inappropriate content (see table above).

Further information can be found at [www.lancsngfl.ac.uk/esafety](http://www.lancsngfl.ac.uk/esafety)

#### **Pupil Access:**

Children are only allowed to access the internet when they are with a member of St. Anne’s Copp CE Primary School , Great Ecclestone staff.

#### **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 ICT manager.

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

Software is installed by the IT Technician or the ICT 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 CE Primary School , Great Ecclestone 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 must be embedded within the curriculum and advantage taken of new opportunities to promote online safety.

Safety across the curriculum and communication:

- Online safety is mentioned regularly in general lessons and each year group has dedicated safety lessons (see Online Safety Policy).
- We teacher online safety once a term across 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.
- Regular online safety updates are passed to staff.
- 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.