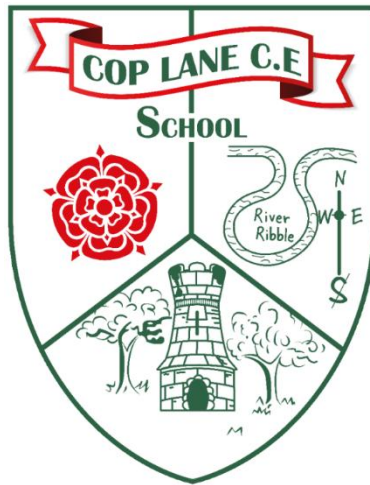


Cop Lane C.E. Primary School



Network and Social Media Policy

September 2026

This policy is embedded in our school's mission statement and distinctive Christian vision:

A welcoming Christian community, committed to one another, giving our very best at all times.

Our church school is a welcoming and caring Christian family where everyone is valued and supported so that they can flourish. We aim to instill a lifelong love of learning and nurture everyone's individual talents. Through Jesus Christ, our aspirations, hopes and dreams can be achieved.

'I can do all things through Christ who strengthens me.'

Philippians 4.13

Purpose

This policy:

- sets guidelines and rules on the use of the school's official social media channels;
- establishes clear expectations for how members of the school community engage online;
- supports the school's Child Protection & Safeguarding Policy and Data Protection Policy;
- applies to social media use for both business and personal purposes, whether during working hours or otherwise, and regardless of whether accessed using school or personal equipment.

It applies regardless of whether the social media is accessed using:

- School IT facilities and equipment
- Equipment belonging to members of staff and pupils
- Any other IT/Internet-enabled equipment

Legal and safeguarding context

This policy should be read alongside the Child Protection & Safeguarding Policy and the school's Staff Code of Conduct. Where social media use gives rise to safeguarding concerns (including child-on-child abuse, online sexual harassment or disclosures), staff must follow the school's safeguarding reporting procedures and inform the Designated Safeguarding Lead (DSL) or a deputy without delay. This policy is written with reference to Keeping Children Safe in Education 2026 (DfE) and UK GDPR.

Definition of social media

For the purposes of this document, 'social media' includes all technologies that allow individuals to communicate and share information (including photos and video). This includes social networks, blogging platforms and group messaging services such as WhatsApp.

Use of official school social media

Official school channels:

- Facebook
- X (formerly Twitter)
- Instagram

Official accounts are owned by the governing body. Access is restricted to authorised staff and administrators; the named administrator is the headteacher. When staff with account access leave, credentials are changed immediately. Content posted via official accounts is the responsibility of the headteacher and the Safeguarding Governor for oversight.

Only authorised staff may manage or post to official accounts. Suggestions for content should be given to the account manager. Staff must follow the procedures below when proposing posts involving pupils.

What we will post

We will post:

Alerts and reminders (procedures, severe weather, events);

- communications about school events and activities;
- job vacancies and volunteer requests;
- links to newsletters and information for parents;
- achievements of pupils and staff (subject to consent);
- photos or posts about trips and activities (see image consent below);
- seasonal greetings and appropriate messages about religious festivals.

Image consent and naming

- We will publish images of pupils only where parents/carers (and where appropriate the pupil) have given explicit written consent.
- We will not publish full names alongside images except where specific parental consent has been given for an identified purpose.
- Staff must not tag or name pupils on social media without explicit permission.
- Parents/carers may withdraw consent at any time by contacting the school office; the school will remove images as soon as reasonably possible.

Moderation and abusive content

Staff responsible for official accounts will remove as soon as reasonably possible:

- abusive, racist, sexist, homophobic or inflammatory comments;
- spam and personal information (telephone numbers, address details);
- posts advertising commercial activity or asking for donations;
- any content we consider a safeguarding risk.

Repeated abusive postings by parents/carers will lead to: (1) a formal written warning from the headteacher; (2) removal or blocking from official pages; and, if necessary, action under the Complaints Policy or platform reporting/legal routes if threats or harassment occur.

Following and liking

- The school will only 'like' or follow pages that are appropriate for the school community. Being liked or followed does not imply endorsement.

Personal use of social media by staff

Staff must:

- act in a manner consistent with the Staff Code of Conduct and safeguarding responsibilities;
- report any safeguarding issues they become aware of immediately to the DSL;
- maintain appropriate privacy and security settings on personal accounts.

Staff must not:

- use personal accounts to conduct school business (except in exceptional, pre-approved situations agreed with the headteacher);
- accept friend requests from current pupils (past pupils only in exceptional, pre-approved circumstances and not for business purposes);
- post images of pupils from personal accounts;
- link personal social media to school email addresses;

- use personal social media during timetabled teaching time except in a professional capacity agreed by the headteacher.

Use of personal devices for images

- Staff must not use personal mobile phones or devices to take or store images or video of pupils unless pre-approved by the headteacher for a documented reason (for example, where school equipment cannot reasonably be used for off-site activity). In exceptional cases the member of staff must transfer images immediately to the school server, delete them from the device and record the transfer. Unauthorised photographing or storing of pupil images on personal devices is prohibited.

Group messaging and parent groups

- Staff must not join or administer parent/pupil WhatsApp or similar groups in a personal capacity. Official communication with parents should use school systems (school email, telephone, official platforms). Staff should not use group messaging apps to discuss pupils or share images.

Online safeguarding incidents

If staff become aware of online incidents involving pupils (cyberbullying, sexual harassment, or making/sharing of nudes/semi-nudes, including AI-generated images), they must:

- not view, forward, download or share any images unnecessarily;
- preserve evidence (screenshots or logs where appropriate) without circulating content;
- secure devices if safe and appropriate to do so;
- report immediately to the DSL who will follow the Child Protection & Safeguarding Policy and national guidance (UKCIS/DfE). Where a criminal offence may have been committed, the DSL will involve the police and local authority children's social care as required.

Pupils' use of social media

Pupils are expected to be respectful online. Pupils must not:

- post or share images of other pupils without permission;
- use social media to target staff, pupils or parents.

Concerns about pupil social media use will be dealt with under the Behaviour Policy and may be escalated to safeguarding procedures if necessary.

Parents/carers' conduct online

Parents/carers are expected to model safe, respectful social media use. They must:

- direct complaints through official school channels so they can be dealt with under the Complaints Policy;
- refrain from posting images of other children without consent; and
- not make abusive comments about staff, pupils or other parents on social media.

Data protection and retention

All social media activity published under the school's accounts is processed in line with the Data Protection Policy and UK GDPR. Content and associated records (permission forms, complaints, moderation logs) are retained in accordance with the Records Management Policy. Personal data processed for publication will be limited to what is necessary and lawful. Monitoring and moderation records are retained for a defined period in line with the school's retention schedule.

Monitoring and legitimate access

The school reserves the right to monitor, intercept and review staff activities using school IT resources and communications systems for legitimate business purposes, including detection and investigation of unauthorised use or safeguarding concerns. Monitoring will be proportionate and lawful.

Account management and governance

Official accounts are managed by authorised staff; the headteacher is the administrator. Governance oversight (Safeguarding Governor) will periodically review content and incidents (anonymised) and ensure compliance with this policy.

Sanctions

Breach of this policy by staff will be managed under the Staff Code of Conduct and may lead to disciplinary action. Pupils' breaches will be dealt with under the Behaviour Policy and may be escalated to safeguarding processes where appropriate.

Related policies

- Child Protection & Safeguarding Policy
- ICT and Internet Acceptable Use Policy
- Behaviour Policy
- Staff Code of Conduct
- Mobile Phone Use Policy
- Records Management and Data Protection Policy
- Complaints Policy

Review

This policy will be reviewed at least annually or sooner in response to lessons learned, changes in statutory guidance (KCSIE) or significant incidents.

This policy was reviewed by Mr I. Ashmore in September 2026.

It will be reviewed again in September 2027 or sooner if needed.

Signed:

I. P. Ashmore