



Carlton VC Church of England Primary School

Social Media Policy 2026

'I am the vine, you are the branches; those that abide in me and I in them will bear much fruit' (John 15:5)

Approved by: Jo Bevis
Staff
Governors

Date:

Written by: Jo Bevis

Date: May 2026

Sourced from: Various Sources

Last reviewed on: May 2026

Next review: June 2027

Contents	Page
Rationale	3
Purpose	3
Scope	3
Principles	3
Responsibilities	4
Account Management	4
Parental Control and Consents	
Content Standards	5
Moderation, comments and engagement	6
Safeguarding	6
Data Protection and GDPR	6
Staff conduct and personal accounts.	7
Third Party Contractor Content	7
Storage, Archiving and Removal	7
Training and Support	8
Monitoring, Evaluation and Review	8
Complaints and Breaches	8
Quick practical rules for staff posting on media	8
Policy links and statutory references (sources)	8
Framework note	9
Appendices	
A: Template for parental consent	10
B: Record of removal of content	10

Rationale

Carlton Church of England Primary is a small rural school that has seen pupil numbers decline for reasons including lower local birth rates. As part of our School Improvement Plan we will therefore take a more proactive approach to marketing to ensure parents in our community and beyond understand what we offer. Using social media will allow us to showcase our strengths — for example our recent Ofsted “Good” judgement, SIAMS Grade 1, strong attendance and broad curriculum — and present a clear, positive picture of life at Carlton to prospective parents.

Purpose

- Promote the school, its achievements and community life to prospective parents and the local community using free public channels (TikTok, Instagram and Facebook).
- Protect pupils, staff and the school’s reputation by setting clear expectations and safe practises for social media use.
- Make sure our online presence reflects The Carlton Way and our Christian vision and values.

Scope

- Applies to all staff, governors, volunteers, contractors and any third-party who posts on behalf of Carlton CoE Primary School.
- Covers official school accounts on TikTok, Instagram and Facebook and any content posted to those platforms.
- Does not replace staff personal social media conduct guidance (see Staff Code of Conduct).

Principles

- Pupil safety and dignity first: no image or personal data of a pupil will be published without explicit parental/carer consent.
- Transparency: accounts will be clearly identified as official school accounts and display our logo, name and our vision statement (The Carlton Way).

- Accuracy and professionalism: posts will be factual, reflect school values, school activities and avoid political campaigning.
- Proportionality: we will only publish images and detail necessary to communicate the message.

Responsibilities

- Headteacher: overall responsibility for content and compliance and maintains account credentials, posts content, approves scheduled activity, oversees consent records and archives.
- DSL (Designated Safeguarding Lead): oversight of safeguarding-related content and immediate escalation point for concerns.
- All teaching staff will have administration rights but will need to be approved by the headteacher before posting.
- Governors: periodic review of policy and social media performance.

Account Management

- Account will be controlled by the headteacher,
- Access to the account for posting will be by teachers and one PTFA member (these are nominated people, if they leave they will be removed immediately).
- Account profile must include: school name, logo, brief vision statement (The Carlton Way), link to school website, contact email/phone.
- Use official school email addresses to administer accounts; never personal emails.
- Passwords: stored securely and changed whenever an authorised staff member leaves.
- Two-factor authentication (2FA) must be enabled.
- Only school-owned devices to be used for capturing and posting pupil images where possible.

Parental Control and Consents

- Written parental consent required at the start of each academic year via the school's media/photography consent form. (see appendix A)

- For any new starters or in-year admissions, collect consent at induction.
- Do not publish photos of pupils where consent is not given.
- If a child who previously consented leaves or withdraws consent, remove future use and where practicable remove existing content (note platform limitations). Record withdrawal date in consent records.
- For any media featuring a small number of pupils (especially 1–2 pupils), do not include identifying information (class/age only), unless explicit consent for naming is given.
- Never tag pupils with names or personal details on public posts.
- Never publish content that reveals precise location metadata (e.g., enable location services off when uploading).

Content standards

- Children's work and images should demonstrate learning, the school's vision and values, and safeguarding best practice.
- Do not post images which could be embarrassing, compromising or which show pupils in vulnerable contexts.
- Avoid publishing images of medical incidents, injuries, safeguarding incidents, confidential information, or sensitive personal data.
- Use neutral captions: class/year group rather than names,
- No commercial endorsements or advertising for third parties on official accounts.
- Do include regular, positive content: school events, pupil achievements, trips, learning displays, newsletters and reminders.

TikTok, Instagram and Facebook specific guidance

- TikTok/Instagram/Tiktok: ensure content is age-appropriate and aligns with school values.
- Do not encourage pupils to create content for the school's account without parental consent and staff supervision. Be cautious with trending audio or challenges - avoid those that could risk safeguarding or reputation.
- Facebook/Instagram/Tiktok: maintain clear moderation of comments and direct messages. Set page messaging preferences to notify

nominated staff. Use privacy settings for admin roles and restrict who can post to the page.

- Reels/short-form videos: obtain specific consent for video before posting. Prefer group shots and classroom-wide images rather than close-ups of individuals where consent is limited.

Moderation, comments and engagement

- Comments: nominate two staff to monitor comments daily on school days. Remove or hide abusive, defamatory, racially abusive or potentially grooming comments and keep a record of any removals and reasons.
- Direct messages: respond via official school email or redirect urgent safeguarding messages to the DSL. Do not provide private contact details of staff or pupils.
- If a parent posts a complaint publicly, remove and acknowledge receipt promptly via email. Keep a record.
- Escalate potential safeguarding concerns raised via social media immediately to the DSL and follow safeguarding procedures (do not investigate via social media).

Safeguarding

- Any safeguarding disclosure or incident reported via social media MUST be logged on CPOMS immediately and referred to the DSL.
- If a staff member suspects online grooming, explicit images, exploitation or criminal behaviour, report to the DSL and contact the police/CEOP as required.
- Maintain records of all public posts, promotional campaigns and any complaints related to social media for at least one year (preferably longer per data retention schedule).

Data protection and GDPR

- Personal data published only where there is lawful basis and explicit consent.

- Keep a secure register of consent linked to each pupil record. Consent forms must state how and where images will be used, which platforms, and how parents can withdraw consent.
- Do not publish personal contact details (phone numbers, email addresses) of pupils or staff.
- Prior to publishing, remove or blur any sensitive information visible in photos (e.g., addresses on displays, pupil medical notes).

Staff conduct and personal accounts

- Staff must not use personal social media accounts to follow, befriend or communicate privately with pupils under 18.
- Staff should separate personal and professional profiles; if staff appear in school posts, they must ensure their own profiles are professional and aligned with the school's safeguarding expectations.
- Staff must seek permission before using pupil images on their personal accounts even if those pupils are their own children.
- Social media use that damages the school's reputation or breaches confidentiality will be dealt with under staff disciplinary procedures.

Third-party and contractor content

- Any third party producing content for the school must sign an agreement that they will adhere to this policy and data protection requirements.
- Contractors must use school-provided consent documentation and follow the same safeguarding and data storage rules.

Storage, archiving and removal

- The school will not store or archive materials used as these can be accessed on the platforms.
- When consent is withdrawn, remove future use and, where possible, delete files and request removal of content from platforms. Record actions taken and dates. See Appendix B.

Training and support

- All staff with posting responsibilities must complete annual refresher training on this policy, KCSIE expectations and GDPR basics at the beginning of the academic year or on induction.
- DSL and Headteacher to receive specific training on online harms, platform moderation and escalation routes.

Monitoring, evaluation and review

- Communications lead to produce a short termly report to SLT and governors showing activity, engagement metrics and any incidents.
- Governor committee (Safeguarding/Standards) to review policy annually and after any serious incident.

Complaints and breaches

- Any breach of this policy must be reported to the Headteacher immediately.
- Breaches may lead to internal investigation and, depending on severity, disciplinary action.
- For complaints from parents/public, follow the school complaints procedure; where content is defamatory or illegal, seek legal advice.

Quick practical rules for staff posting on media

1. Use only school accounts and devices.
2. Check the parental consent register before selecting any images.
3. Two-person sign-off for posts featuring pupils.
4. No pupil names, no location tags, no close-up shots of individual pupils without explicit naming consent.

Policy links and statutory references (sources)

- Keeping Children Safe in Education (Department for Education).
- Data Protection Act 2018 & UK GDPR.
- School Information (England) Regulations 2008 (as amended).

- DfE guidance on online safety and staff/pupil online conduct.
- Data Protection Policy
- Safeguarding Policy
- Communications and Code of Conduct for Parents Policy

Framework note

- This policy supports the school's approach to Personal Development and Safeguarding under the OFSTED framework and helps evidence how the school keeps pupils safe online.