Diocese of Carlisle — Social Media Policy

Date: March 2026

Applies to: DBF employees, office holders, authorised volunteers and contractors acting on behalf of the Diocese of Carlisle.

Related documents: Annex A (Digital Safeguarding — Recommended Procedures); Annexes B–H (good-practice and operational guidance).

1. Introduction & Principles

1.1 Purpose

This policy sets mandatory standards for the official use of social media when acting for the Diocese of Carlisle, protecting people, data, and reputation while enabling confident digital engagement.

1.2 Scope

This policy applies to all diocesan social media activity by DBF employees, office holders, authorised volunteers and contractors when acting in an official capacity. It covers:

- **Channels**: Official diocesan accounts and ministry brands (e.g., Network Youth Church, Northern Young Leaders Project, Pioneers, other CDBF-run accounts).
- **Personal accounts used for work**: Any personal account used to conduct diocesan business, represent a diocesan role, or publish diocesan content.
- **Activities**: Posts, comments, replies, stories/reels, DMs/group chats, live streams, events, ads, and community moderation.
- **Tools & devices**: Third-party tools used to plan/publish/monitor/archive content; and any device used to access diocesan accounts.

Exclusions/overlap

- Purely private, non-diocesan use of personal accounts is out of scope unless it references diocesan work or creates a reasonable link to your role.
- Parish/school/charity partners should apply their own policies; where both apply, the stricter control should be followed.
- This policy applies regardless of location (UK or abroad) when representing the Diocese online.

1.3 Terms used in this policy

- MUST — Mandatory requirement. Any deviation requires prior written approval from the Diocesan Head of Communications; where safeguarding or data protection is affected, also from the Diocese Safeguarding Officer (DSO) / Data Protection Officer (DPO).
- SHOULD — Strong recommendation. An alternative is acceptable only if you record a brief risk assessment and rationale, and tell your manager if material.
- MAY — Optional guidance to support good practice.
  Note: MUST NOT and SHOULD NOT are the corresponding prohibitions.

1.4 Principles

- **Lawful & transparent**: follow UK law and platform terms; identify your role on diocesan business.
- **Safeguarding first**: follow Annex A (with Annex C/D where relevant).
- **Reputation**: don't post in a way that could bring the Diocese/DBF into disrepute.
- **Data responsibility**: see Section 3.
- **Pastoral tone**: accurate, fair, courteous.
- **Records**: keep proportionate logs of key decisions and incidents (see 2.8/4).

2. Policy Requirements

2.1 Safeguarding

- DBF employees and authorised volunteers MUST follow Annex A: Digital Safeguarding — Recommended Procedures for any contact with, or content about, children, young people, or vulnerable adults.
- Where a parish policy is stricter, the stricter control applies. When in doubt, consult the DSO.
- You MUST escalate any safeguarding concern immediately to the DSO (and 999/CEOP where appropriate).
- Safeguarding concerns may include risks of radicalisation or exposure to extremist content online. Where such concerns arise they should be treated as safeguarding matters and escalated through diocesan safeguarding procedures in line with the UK Prevent strategy.
- For practical rules on channels, DMs, minimum ages and consent, see 2.6 and Annexes A (procedures), C (minimum ages), D (media/consent).

  .

2.2 Conduct & Disrepute

Users MUST NOT post, comment, message, or engage in a way that reasonably risks bringing the Diocese or DBF into disrepute. This clause regulates conduct, not theological viewpoint or lawful expression.

Prohibited conduct includes (not exhaustive):

Employees must not do any of the following:

- High-volume or aggressive posting that appears harassing, baiting, or vexatious.
- Personal attacks, insults, or demeaning language toward individuals or groups.
- Sharing unverified allegations, doxxing, or posting confidential/inside information.
- Hate speech, extremist content, discrimination, or material that undermines a safe church culture.
- Offensive or obscene material on accounts linked to diocesan roles.
- Bypassing moderation (e.g., creating new accounts to evade blocks) or encouraging pile-ons.
- When in doubt: pause, seek advice from the Head of Communications before posting. You must always use the agreed spokesperson for public statements or media comment.

2.3 Law, Regulation & Platform Terms

- MUST comply with UK law (defamation, harassment, privacy, copyright, data protection) and each platform's Terms of Service before posting.
- MUST remove/disable unlawful or harmful content promptly and escalate per Section 4.
- MUST respect copyright/licensing: use only owned/licensed media; credit where required.
- MUST handle personal data per Section 3; involve the DPO where needed (e.g., Data Protection breaches, rights requests).
- MUST follow elections & political activity guidance from national church bodies and the Charity Commission; official channels must not engage in party-political campaigning.
- MUST make advertising/endorsements transparent (e.g., "Ad", "Gifted", "Partner") and keep a simple record of any consideration received.
- SHOULD use platform safety features (moderation, reporting, age limits) and document significant takedown/block decisions.

2.4 Account Governance

MUST

- Each official account has a named owner and at least one backup admin.
- Use diocesan-managed email/phone for account recovery and enable multi-factor authentication (MFA) on all admin logins. (See Annex F.)
- Keep an up-to-date admin/access list; remove access immediately on role change or exit and complete a handover.

- Store credentials only in an approved password manager; never share passwords by email, chat, or documents.
- Maintain an Account Register (account name/URL, purpose, owner, admins, recovery method, MFA status, archiving approach, third-party tool access).
- Use role-based permissions (editor/moderator/analyst) rather than sharing a single login.

SHOULD

- Review admin access and the Account Register quarterly; test recovery options.
- Use diocesan service inboxes (e.g., comms@…) for ownership.
- Restrict third-party tools to least privilege; remove unused integrations.
- Label bios with a short purpose and a contact route; keep branding consistent.
- For youth-facing accounts, include: **"Report online abuse to CEOP: ceop.police.uk"** and a DSO contact. (Full template in Annex D.)

2.5 Content Standards

- MUST have appropriate consent before publishing identifiable images/video/audio. (Ref: Annex D)
- MUST NOT publish a child's full name with a clear image unless there is explicit parental consent and a documented justification.
- MUST NOT publish special category personal data (UK GDPR) without a lawful basis, necessity test, and DPO sign-off where required. (Ref: Section 3)
- MUST use only owned/licensed media; credit where required.
- MUST manage location safety (avoid sensitive locations; strip geotags/delay posts).
- MUST NOT store or forward illegal images; preserve evidence and escalate per Section 4/Annex A.
- SHOULD label AI-generated/edited media where material to interpretation; add ALT text/captions; correct errors promptly.

2.6 Communications with Under-18s

MUST

- MUST Follow Annex A/C for approved channels, visibility, group messaging, and logging. These include:
    - Keep communications visible and accountable (two-adult rule).
    - Avoid 1-to-1 DMs; if unavoidable for immediate safety, keep brief/factual and log it.
    - Under-13s: no direct DMs; route via a parent/guardian.
    - Use only church/diocesan-managed accounts; do not use personal profiles or phone numbers.
    - Do not use disappearing/secret messages for ministry communications.
    - Obtain consent for participation in digital groups and for media (see Annex A/D).

- Escalate immediately to the DSO if concerned; preserve evidence.

Visibility on public channels

- MUST treat a young person's comment on a public post as public (handle + text visible), even if their account is private.
- SHOULD encourage under-18s who engage with diocesan channels to keep personal accounts private and avoid posting identifying details (e.g., school, routine, phone, address) in public comments.

Following & contact

- MUST NOT follow personal accounts of under-18s from official channels.
- MUST keep conversations in visible, auditable spaces (two-adult rule). Do not move to 1-to-1 DMs except for immediate safety, and log if that happens (see Annex A).

Moderation & records

- MAY hide/remove youth comments that could identify a young person or create risk; SHOULD follow up via a safer route (parent/guardian or group space).
- SHOULD keep a brief moderation note (date/time, handle, gist, action) and email the Digital Support Enabler / Support Centre for tracking.
- SHOULD Set contact hours and typical reply times.
- SHOULD Keep proportionate records; if messages auto-delete, note date/time, participants, gist.

2.7 Moderation & Escalation

- MUST moderate proportionately. Unlawful/harmful content must be removed/hidden and escalated per Section 4.
- SHOULD use hide/mute before block where appropriate; MAY block repeat or egregious offenders (see Annex B).
- MUST preserve evidence (URLs, screenshots, timestamps) before/while taking action.
- MUST refer all media enquiries to the Communications Lead.
- MUST treat threats/safeguarding concerns as incidents: Contact DSO (and police/CEOP where appropriate).
- SHOULD keep a brief moderation log (what/when/why; user ID).

2.8 Records & Retention

- SHOULD Keep a simple, auditable record of significant official communications and moderation decisions where proportionate to risk.
- SHOULD If a platform auto-deletes messages, make a brief note or screenshot at the time capturing date/time, participants, and the gist of the exchange.
- MUST Store securely and apply the diocesan retention schedule (see Section 3).

- MUST If records contain personal data or become part of an incident, notify the DPO and follow Section 4.

2.9 Training & Competence

- MUST complete diocesan social media and safeguarding training appropriate to role (see Annex H) before administering an account or communicating with children/young people/vulnerable adults.
- MUST record completion in the team's training log; managers are responsible for keeping records up to date.
- SHOULD seek further training and support from the Digital Support Enabler as required for the role.

3. GDPR / Data Protection (summary)

- MUST Lawful basis: Identify and document the lawful basis for each activity (e.g., legitimate interests, consent for optional media use). If processing special category personal data (e.g., health, religion), record the Article 9 condition and any additional safeguards.
- MUST Transparency: Link to the diocesan privacy notice where appropriate and honour withdrawal of consent.
- MUST Data minimisation & security: Collect/store only what's necessary; protect it with MFA, access controls and secure storage. Avoid exporting platform data unless needed.
- MUST Rights requests: Route Subject Access, erasure or objection requests immediately to the DPO; do not delete data under request without DPO advice.
- MUST Breach: Suspected personal-data breaches (mis-send, lost device, exposed inbox, hacked account) must be reported at once per Section 4.
- SHOULD International transfers: Be aware platforms may store data outside the UK; where exporting data off-platform, check transfer safeguards with the DPO.
- MUST Children's data: Apply extra care to under-18s; default to least data, parent/guardian involvement, and clear consent for media (Annex A/D).

4. If Something Goes Wrong (Incidents & Escalation)

4.1 Safeguarding

- MUST If you have any safeguarding concern, stop the activity, follow Annex A, and notify the Diocesan Safeguarding Officer (DSO) immediately.
- MUST If there is immediate risk of harm, call 999. For online child abuse/exploitation concerns, report to CEOP as advised by the DSO.
- MUST Preserve evidence (URLs, screenshots, timestamps). Do not download, store, or forward illegal images; note what was seen and where.
- MUST Secure accounts if relevant (reset passwords, revoke sessions).
- SHOULD Inform your line manager and make a brief incident record (what, when, who, action taken).

4.2 Operational incidents

Examples include: impersonation, account compromise/hack, doxxing, serious harassment, defamation risk, illegal content, major pile-on, data exposure.

- MUST preserve evidence: capture URLs, screenshots, and timestamps before/while taking action.
- MUST secure accounts: reset passwords, revoke active sessions, verify/enable MFA, remove unknown admins/apps.
- MUST escalate immediately to the Communications Lead. If personal data may be involved, inform the DPO at once.
- MUST pause public replies until a response is agreed; use one authorised spokesperson only.
- MUST use platform reporting tools (impersonation/abuse/illegal content) and pursue legal escalation where advised.
- SHOULD assess safety risks; if threats are credible or a crime may have been committed, contact police (and CEOP where child-safety is in scope).
- SHOULD keep a brief incident log: what happened, when, accounts affected, actions taken, who was informed, next steps.

5. Contacts

Role	Name	Email	Phone
Diocesan Safeguarding Officer (DSO)	Jo Van Lachterop	Safeguarding.adviser@carlislediocese.org.uk	07458 016884
Diocesan Head of Communications	Dave Roberts	Communications@carlislediocese.org.uk	
Data Protection Officer (DPO)	Ali Ng	Ali.ng@carlislediocese.org.uk	
Digital Support Enabler	Rob Humphreys	Robert.humphreys@carlislediocese.org.uk	

Annex A — Digital Safeguarding: Recommended Procedures

Use alongside your parish safeguarding policy. Where parish policy sets stricter controls, the stricter control applies.

Approved Channels & Visibility

- Use official, auditable channels for ministry communication. Do not use personal accounts for 1-to-1 with children/young people.
- Group messaging includes at least two approved adult leaders; for under-13s, include parents/guardians where feasible.
- Avoid private 1-to-1 DMs with under-18s. If unavoidable for immediate safety, keep brief and factual, move to a safer channel quickly, and record the interaction.
- Do not create secret/closed groups that exclude oversight.
- Keep contact lists and group membership up to date.
- Youth-facing accounts SHOULD signpost safeguarding help in bios, including: "Report online abuse to CEOP: ceop.police.uk" and a DSO contact.

Consent & Communication Boundaries

- Obtain parental/guardian consent for under-18 participation in digital groups, including permissions for images/video; renew annually for ongoing groups.
- Set contact hours (e.g., not after 9pm except emergencies) and say replies aren't instant.
- Keep pastoral advice within role boundaries; do not provide counselling beyond training/competence.
- Share only information necessary for ministry purposes.
- Be clear, kind and concise; avoid sarcasm/shaming or language that could be misread.

Photos/Video of Children & Young People

- Collect consent appropriate to context; renew annually for ongoing groups.
- Avoid naming children in captions; never post a full name with a clear image without explicit parental consent and a clear justification.
- At events, display photography/streaming signage and offer a clear opt-out (e.g., wristband/check-in note).

Live Streams & Online Events

- Complete a simple risk assessment; assign roles (host, moderator, safeguarding contact).
- Moderate chat; disable private messaging with under-18s; remove unlawful/harmful content swiftly.

- Use a short broadcast delay where helpful; avoid showing personal data on screen (e.g., addresses, phone numbers).
- Announce if recording; share house rules upfront.
- Keep a brief log of significant moderation actions (e.g., removals/blocks for serious issues).

Minimum Ages & Platform Terms

- Follow platform minimum ages and Terms of Service (see Annex C).
- Do not encourage under-age platform use.
- In mixed-age groups, set rules suitable for the youngest participants.

Record-keeping

- Keep proportionate records of group membership, key decisions, and incident escalations.
- If messaging platforms auto-delete, capture a brief record after significant interactions (date/time, participants, gist).

Reporting & Escalation

- If you think a child is at risk, contact the DSO immediately and consider CEOP/police as appropriate.
- Preserve evidence (URLs, screenshots, timestamps); do not forward indecent images. Follow DSO guidance on secure handling.

Annex B — Social Media Good Practice (Tone, Moderation, Engagement)

Tone & voice

- Be human, pastoral, and clear; avoid sarcasm and pile-ons.
- Use plain English; explain acronyms on first use.
- Keep personal opinions separate from official statements.

Authenticity

- Show real ministry: people, places, and moments as they are (with consent).
- Prefer original photos/video over generic stock; credit creators when you use third-party media.
- Say what you know first-hand; link sources for facts or claims.
- Disclose edits: label AI-generated or heavily edited visuals if it affects how content is understood.
- Avoid over-polish; a simple, truthful post is better than a glossy one that feels staged.
- Correct mistakes openly and quickly; add an edit note if you change a live post.
- Use real names/titles for spokespeople and quote them accurately.

Engagement

- Acknowledge fair criticism and signpost to more detail when useful.
- Correct misinformation politely and include a source link where possible.
- Set expected response times in a bio or pinned post if helpful.

Moderation (day to day)

- Use hide/mute for borderline comments; remove unlawful or harmful content.
- Block repeat or egregious offenders (thresholds are in Section 2.7).
- Apply house rules consistently and avoid back-and-forth arguments.

Moderator quick workflow

1. Spot a youth comment on a public post.
2. Check risk: does it reveal identity/routine/location?
3. Action: hide/remove if risky; avoid public back-and-forth.
4. Follow-up: continue in the group space or via parent/guardian with a short pastoral note.
5. Record: log date/time, handle, gist, action; email the Digital Support Enabler / Support Centre for tracking

Accessibility

- Add ALT text to images and captions to videos.
- Provide a short text summary or transcript for key videos.
- Use CamelCase in hashtags (e.g., #GodForAll).

Content craft

- Use descriptive headlines, front-load key information, and include a clear call-to-action.
- Avoid posting precise locations/timetables that could create risk.
- Review scheduled posts after major news events.

Example house rules (paste on channels)

- Be respectful — no personal attacks, hate speech, doxxing, or illegal content.
- Stay on topic — off-topic or repeated promotional posts may be removed.
- We moderate and may block repeat offenders.

House rules (youth-facing channels)

- Be kind and stay on topic.
- Under-18s: for your safety, please keep your account private and don't post personal details (school, routine, phone, address).
- We may hide or remove comments that could identify a young person or create risk, and we'll follow up through a safer route.
- Safeguarding concerns: contact the DSO. Report online abuse to CEOP: ceop.police.uk.

(For mandatory requirements, see main policy Section 2.7.)

Annex C — Platforms, Outreach & Minimum Ages

Minimum ages reflect platform terms. Do not encourage under-age use.

Platform	Minimum age	Notes
Facebook	13	Pages/Groups for parishes; events; moderation tools available.
Instagram	13	Photos/reels; stories; DM rules apply.
WhatsApp	13	Use for adult teams; avoid 1-to-1 with under-18s; prefer broadcast lists; archive decisions.
TikTok	13	Short-form video; use comments moderation filters.
YouTube	13	Long-form video/live; set 'made for kids' only when appropriate.
Snapchat	13	Transient messages; generally not suitable for youth ministry comms.
X (Twitter)	13	Public posts; consider brand risks; limited DM controls.
Discord	13	Server moderation needed; roles/permissions; audit logs.
BeReal	13	Not recommended for official comms; privacy considerations.
Twitch	13	Streaming; chat moderation essential.

General rules

- Always follow platform Terms of Service and safety controls.
- Use church/diocesan-managed accounts; avoid personal profiles/numbers.
- Keep youth comms visible and accountable (two-adult rule); see Annex A.
- Review this annex annually or when major platform changes occur.

Platforms note (visibility)

- A private account protects your profile/media, not your comments.
- Comments made on public posts are public (handle + text visible).
- Prefer posting from private accounts and avoid sharing identifying details in comments.

- Use group spaces (two-adult visibility) rather than public threads for longer conversations.

Annex D — Account Set Up & Administration

Account naming & bios

- Name accounts clearly: *Diocese/Parish + ministry*.
- Bios include: a short **purpose**, a **safeguarding contact route**, and house rules.
- **Youth-facing bios include: "Report online abuse to CEOP: ceop.police.uk"** and DSO contact details.

Bio/description template (youth-facing)

- *Purpose:* "Updates from [Parish/Ministry] youth in [Area]."
- *Safeguarding:* "Safeguarding concerns? Contact the **Diocesan Safeguarding Officer**: [email/phone]. **Report online abuse to CEOP:** ceop.police.uk."
- *House rules:* "Be respectful; no personal attacks or illegal content. We may moderate."

Brand & visibility

- Use diocesan brand assets correctly; keep names, logos and tone consistent across platforms. See godforall.org.uk/logos and carlislediocese.org.uk/logos
- Link to a single **About/Link-in-bio** page that repeats safeguarding and CEOP information.

Access & handover

- On role change/exit: remove access immediately; reset passwords/MFA; review page roles and third-party tools; update bios/contact details; record handover in the Account Register.

Protecting Young Followers on Public Accounts

- Encourage under-18 followers to use private accounts and avoid sharing identifying details.
- Admins should avoid viewing or engaging with personal profiles beyond what is necessary for moderation.
- If a young person's public profile shows concerning or identifying information, follow the moderation and safeguarding escalation pathway.
- Do not follow back personal accounts of under-18s.
- Add a periodic safety reminder post encouraging all followers to check privacy settings.

Photography & Filming – Consent Guide

This table provides guidance on when consent is required for photography and videography within a church context, in line with UK GDPR and Church of England best practice.

Key rules

- Do not post a **child's full name with a clear image** without **explicit parental consent** and a clear justification.
- Use **signage and announcements** at services/events; provide **photo-free seating**.
- Treat sensitive contexts (baptism, funeral, crisis) as **consent-only**.
- Keep consent records; **renew annually** for ongoing groups/roles.
- Take photographs/videos of those **you do** have consent for.

Scenario	Who's in the image	Use of the image	Consent needed?	Lawful basis & good practice
Wide shot of a congregation during worship or event	Adults in crowd, not individually focused	Website, social media, newsletter	❌ No written consent (OK with clear notice)	Rely on legitimate interests. Display signs at entrance, make an announcement, and offer an opt-out area.
Four adults sitting or standing together during church service	Recognisable adults	Social post, website photo, noticeboard	⚠️ Written consent needed if general context	Still 'legitimate interests.' Must have photo notice and opt-out. Avoid private/sensitive moments.
A posed group photo (e.g. PCC, choir, volunteers)	Identifiable adults	Website, social, printed materials	✅ Written/electronic consent recommended	You've arranged the photo intentionally, so treat it as explicit consent.
Individual portrait or story (e.g. testimony, volunteer feature, interview)	One adult named or quoted	Website, social media, printed materials	✅ Written/electronic consent required	Explicit consent needed — they're being featured and named.
Child or young person identifiable	Anyone under 18	Any public use	✅ Written parental consent required	Always explicit consent from someone with parental responsibility.
Crowd including children (e.g. all-age service, holiday club)	Mix of adults & children	Website or social	⚠️ Avoid if possible, or crop/blurry children	Use signs and announcements. Get parental consent if a child is recognisable.
Livestream or recorded service	Congregation visible in background	YouTube/Facebook stream	⚠️ Signage + announcement required	Inform all attendees. Provide photo-free seating. Avoid close-ups without consent.
Choir, band, or service leaders (regularly on camera)	Adults in role	Livestreams, videos, website	✅ Explicit or ongoing recorded consent	Use a standing consent form reviewed yearly, or record them giving consent on video.
Baptism, confirmation, wedding, funeral	Individuals/families in sensitive context	Public social or printed	✅ Explicit consent required	Sensitive moments — never assume consent.
Internal church newsletter only (not online)	Known congregation members	Printed newsletter for members	⚠️ Implied consent acceptable if expected	Still honour opt-outs and remove on request.

Filming for external media (press, TV, partner organisation)	Anyone identifiable	External publication	✅ Explicit written consent required	You'll be sharing outside church control — written permission essential.
Anonymous back-of-head or silhouette shots	Unidentifiable people	Any use	❌ No consent needed	No personal data being processed.

Safety & storage

- Store consent records securely and link them to the media asset/use.
- Remove content on legitimate request where consent is withdrawn and no overriding lawful basis applies.
- Do not post images that reveal sensitive personal data (health, pastoral crises) without a clear lawful basis and DPO advice

Annex E — Photos & Video, AI & Deepfakes

1) Consent & identification

- Get consent before publishing identifiable images/video/audio; keep a record linked to the asset.
- Do not publish a child's **full name with a clear image**.
- Use **event signage** and a short announcement where filming/photography is likely. Provide a **photo-free area**.
- If consent is withdrawn, take down the content promptly unless there is a clear overriding basis (check with the DPO/DSO as needed).

Signage template (paste to posters/slide):

Photos/video may be taken and used on our channels. Please speak to a steward if you prefer not to be included. Photo-free seating available. Safeguarding concerns: contact the DSO. Report online abuse: **ceop.police.uk**.

2) Sensitive contexts

- Treat baptisms, confirmations, weddings, funerals, pastoral crises, hospital/home visits as **consent-only**.
- Avoid images that disclose health, financial hardship, or other special-category data without DPO advice.

3) Copyright & credit

- Use only media you **own** or are **licensed** to use; keep licence proof.
- Credit creators where the licence requires it.
- Keep third-party logos/brand assets within their usage rules.

4) Location & safety

- Strip **geotags** from images/video before posting when exposing individuals.
- Avoid broadcasting private addresses, schools, or predictable routines.
- Delay posting from private homes or locations that could create risk.

5) Filming & livestream tips

- Assign roles: **host**, **moderator**, **safeguarding contact**.
- Avoid close-ups of children unless consented; frame wide.
- Moderate chat; remove unlawful/harmful content and keep a brief log (what/when/why).
- Announce if recording; link to privacy notice where appropriate.

6) AI-generated or AI-edited media

- Don't fabricate people or events.

- If AI materially affects how content may be understood, **label it**.

Disclosure line (caption example): *Image created/edited with AI for illustration.*

- Keep originals and version history.
- Avoid using AI tools that claim broad rights over uploaded images unless necessary and approved.

7) Spotting fakes & deepfakes (quick checks)

- Look for artefacts: warped text, hands/ears, lighting and shadow inconsistencies, mismatched reflections.
- Check **context**: does the setting, weather, signage, or uniforms make sense?
- Run a **reverse-image search** on key frames/stills.
- Compare against known authentic sources; check timestamps/EXIF where available.
- If in doubt, **don't post**; ask the Communications Lead for a verification call.

8) Safety: illegal content

- Do **not** store or forward suspected illegal images of children.
- Note what was seen and where; **preserve evidence** via URLs/screenshots of pages (not the image itself) and escalate immediately per Section 4 / Annex A.

9) Storage & retention

- Store consent forms and media in approved locations; link the consent record to the asset.
- Apply the diocesan **retention schedule**; set review dates for older galleries and livestream archives.
- Remove access for leavers; keep an audit trail of edits/takedowns.

10) Captions & credit (quick pattern)

- **Who/what, where, when** (avoid full names of children).
- Credit: "Photo/Video: [Name]" if required by licence.
- Add **ALT text** for accessibility (describe the scene, action, and any text in the image).

Annex F — Virtual Meetings & Live Streams

1) Pre-event setup

- Do a simple **risk assessment** (who's in shot, camera angles, chat risk).
- Assign roles: **host**, **moderator**, **safeguarding contact**.
- **Test the tech** (audio levels, camera framing, captions).
- Set **house rules** for chat/comments and agree who can pause/stop the stream.
- Prepare **no-film seating** and camera positions that avoid wide pans of the congregation.

2) Inform people clearly

- **Signs at entrances** (paste text below).
- **Verbal reminder** at the start; point out no-film seating and stewards.
- Link or QR to the **privacy notice**.

Signage text (paste):

This service is being live-streamed/recorded. No-film seating is available. Privacy notice: [link/QR]. A steward can help. Safeguarding concerns: contact the **Designated Safeguarding Lead**. Report online abuse: **ceop.police.uk**.

3) Children and vulnerable adults

- Aim **not** to film children at all.
- If a child could be identifiable (close-ups, distinctive features, solos/readings), obtain **written parental/guardian consent in advance** or adjust the camera so they are **not in shot**.
- For groups (choir/brigades), keep a simple **consent list** and seat "no-image" children in the **no-film** area.
- Do **not** overlay children's names on the stream. Avoid zooming on identifiable minors.

4) During the event

- Keep framing on **clergy/lectern/choir**; avoid congregation pans.
- Use a **short delay (10–30s)** if your setup allows, so you can cut the stream if something sensitive happens.
- **Moderate chat** (hide/remove illegal or harmful content; escalate per Section 4).
- Avoid displaying **personal data** on screen (addresses, phone numbers, prayer lists with sensitive detail).

5) After the event

- Store recordings per the **retention schedule** (e.g., **3–6 months**).
- Keep a **one-page note** of lawful basis (usually **legitimate interests**) and key mitigations (camera angles, signage, no-film seating, child consent where used).
- Log any **incidents and actions** taken (time, what happened, who was informed).

6) Privacy notice (what to include)

- That **live streaming/recording** may occur and typical locations/channels.
- The **lawful basis** and **retention period** for recordings.
- How to **opt out**, request **no-film seating**, or raise concerns.
- Contact routes for the **DSO** and **DPO**.

7) Quick checklist (print for the vestry)

- Cameras framed to avoid congregation ✓
- No-film pews signed and visible ✓
- Entrance/nave signs up; QR to privacy notice ✓
- Verbal reminder delivered ✓
- Child consents checked / no-image children seated ✓
- Moderator logged in (if necessary); house rules set ✓
- Delay enabled (if available) ✓
- Post-event: recording stored, log updated, incidents noted ✓

Annex G — Security (Accounts, Devices, Access)

Accounts & logins

- Turn on **Multi-Factor Authentication (MFA)** for all admin logins (authenticator app preferred over SMS).
- Use a **password manager**; create **unique** passwords for every account.
- Avoid shared logins; use **role-based access** (owner/admin/editor/moderator).
- Review admins **quarterly**; remove leavers immediately and record the handover in the Account Register.
- Check **active sessions** and logged-in devices; sign out unknown sessions.
- Set **recovery email/phone** to diocesan addresses/numbers, not personal ones.

Devices

- Keep OS and apps **up to date**; enable **auto-updates**.
- Turn on **disk encryption** (BitLocker/FileVault) and a **screen lock** (PIN/biometric).
- Separate work and personal profiles where possible.
- Don't store passwords or access tokens in notes, docs, or browsers without the manager.

Email & domains

- Protect the **email inbox** tied to social accounts with MFA.
- Watch for **phishing**: check sender, hover links, verify urgent requests by phone/Teams.

Third-party tools

- Map all tools connected to each platform (schedulers, analytics, link-in-bio, ad managers).
- Grant the **minimum permissions** needed; remove unused apps/integrations.
- Keep a note of who can access **ad accounts** and payment methods.

Backups & recovery

- Keep copies of **brand assets** (logos, templates, fonts) and a list of **official accounts** in a shared diocesan drive.
- Store the **Account Register** alongside a simple **incident sheet** (who to call, where the passwords/MFA codes are, how to revoke access).
- Record **backup admins** and how to contact them out of hours.

Lost/stolen device (quick actions)

- **Revoke sessions** for social and email accounts.
- **Change passwords** and require re-login everywhere.
- **Invalidate app passwords/API tokens** in connected tools.

- Tell the **Communications Lead / IT**; make a short incident note (time, device, accounts affected).

Travel & shared use

- Avoid logging into admin accounts on **public/shared computers**.
- If you must, use a private window, a hardware security key if available, and **log out**; clear cookies.
- Don't approve MFA prompts you didn't initiate (report **MFA spam** to IT).

Advertising & payments

- Keep card details in the platform's **Business/Ad account**, not on a personal profile.
- Restrict who can create or approve ads; review spend alerts monthly.

End of role checklist

- Transfer page/channel **ownership** to the diocesan account.
- Remove the leaver from page roles, ad accounts, and third-party tools.
- Rotate shared credentials and **reset MFA** if the device/token belonged to the leaver.
- Update bios/contact lines if they named the leaver.

Security quick check (monthly)

- Admin list current ✓
- MFA on all admins ✓
- Unknown sessions removed ✓
- Third-party apps reviewed ✓
- Account Register updated ✓
- Incident sheet present & current ✓

Annex H — Training (Who needs what)

Role	Training	Refresh
Account owner/admin	Social media policy overview; safeguarding basics; GDPR basics; security (MFA/password manager).	Every 2 years or on major change.
Youth/NYC leaders	Digital safeguarding (Annex A); consent & media; platform safety.	Annually.

Glossary of Terms

Account Register
A central record of all official diocesan social media accounts, including owners, admins, recovery details, MFA status and purpose.

Admin / Administrator
A person with elevated account permissions who can publish content, change settings, add/remove users and manage security.

AI-generated media
Images, video or audio created or significantly altered using artificial-intelligence tools.

ALT text
A short written description of an image added for accessibility and screen-reader use.

Article 9 data
Sensitive “special category” data under UK GDPR (e.g., health, ethnicity, religion) which requires additional safeguards.

Authorised volunteer
A volunteer formally approved to act on behalf of the Diocese in a defined role.

Backup admin
A second administrator with full access, used if the main owner is unavailable.

CEOP
Child Exploitation and Online Protection Command. The UK national body for reporting online child-safety concerns.

Charity Commission guidance
Rules governing charity conduct, including restrictions on political activity and communication.

Confidential information
Information not intended for public release, including internal documents, personal data and sensitive organisational details.

Consent (media)
Permission—usually from a parent/guardian for under-18s—allowing identifiable images, video or audio to be published.

Data breach
Any incident where personal data is lost, disclosed, accessed or shared unlawfully or by mistake.

Data minimisation
Collecting and storing only the minimum personal data required to fulfil a specific purpose.

Data Protection Officer (DPO)
The diocesan officer responsible for UK GDPR compliance and managing data-protection incidents.

Direct message (DM)
A private, one-to-one or small-group message within a social media platform.

Disappearing messages
Messages that auto-delete or vanish (e.g., WhatsApp disappearing mode). Not permitted for ministry communication.

Disrepute
Actions or posts that could reasonably damage the reputation of the Diocese or DBF.

Doxxing
Publishing private or identifying information about someone without their consent.

Escalation
Reporting an incident or concern to the appropriate diocesan lead (Communications Lead, DSO, DPO).

Evidence preservation
Capturing screenshots, URLs and timestamps before removing content to support safeguarding or legal processes.

Group messaging
Communication within a group chat where visibility and the two-adult rule apply.

Harmful content
Material that risks causing physical, emotional, reputational or safeguarding harm, even if not illegal.

Impersonation
Creating a fake account or profile pretending to be the Diocese or someone associated with it.

Incident log
A brief written record of what happened, actions taken, and who was informed.

Legitimate interests
A lawful basis under UK GDPR allowing processing where needed for diocesan purposes and not overridden by individual rights.

Media enquiry
A request from a journalist or news outlet, which must be referred to the Communications Lead.

Minimum age requirements
Platform rules (e.g., 13+) combined with diocesan safeguarding requirements for online interaction.

MFA (Multi-Factor Authentication)
A login method requiring an additional security step such as a verification code.

Moderation
Managing comments, posts, replies or messages to keep online spaces lawful, safe and respectful.

Official account
A social media channel created or used to represent the Diocese or a diocesan ministry/brand.

Personal account used for work
A personal profile used to carry out diocesan duties or publish diocesan content, bringing it within scope of this policy.

Platform safety features
Built-in tools such as block, mute, hide, comment filters and reporting mechanisms.

Private use (out of scope)
Social media activity that is fully personal and unrelated to diocesan roles, unless it references diocesan work.

Public statement
Any comment made on behalf of the Diocese, requiring use of the authorised spokesperson.

Recovery method
The email, phone number or security tool used for password resets or account recovery.

Retention schedule
Rules defining how long different data and records must be kept before deletion.

Safeguarding concern
Any worry about the safety or wellbeing of a child, young person or vulnerable adult—online or offline.

Screenshots with timestamp
Images captured to document online interactions for evidence and safeguarding records.

Special category personal data
Sensitive data requiring an Article 9 lawful basis, including health information, ethnicity and religion.

Spokesperson
An authorised individual who speaks publicly for the Diocese.

Subject Access Request (SAR)
A formal request from an individual asking to receive the personal data held about them.

Two-adult rule
A safeguarding standard requiring that communication with under-18s is visible to at least two approved adults.

UK GDPR
The UK's data-protection legislation, governing how personal data must be handled.

Unverified allegations
Claims presented without supporting evidence; sharing them is prohibited.

Vexatious behaviour
Aggressive, excessive or bad-faith communication intended to provoke or harass.