Safeguarding
KILLALOE

DIOCESE OF KILLALOE

Social Media Policy & AI Guidance

Safe • Respectful • Accountable • Faith-centred

Original publication: October 2016 | Updated: October 2026

Contents

A simple route through the policy

1.0	Introduction
2.0	Using social media with young people and vulnerable adults
2.1	Facebook / Messenger
2.2	X and similar platforms
2.3	Instagram
2.4	Snapchat
2.5	WhatsApp
2.6	TikTok
2.7	YouTube
3.0	Artificial Intelligence (AI): best practice
4.0	General social media guidelines
5.0	Useful websites, legislation and diocesan policies

1.0 Introduction

The Diocese of Killaloe recognises the impact, involvement and influence that social media platforms such as Facebook, X, TikTok, Snapchat and Instagram have on the lives of adults and young people under 18. We also acknowledge the role these platforms play in how young people interact with one another.

Used appropriately, social media can help Parishes and Youth Ministry deepen relationships, encourage faith, promote opportunities and events, and communicate positively about the work of the Diocese of Killaloe.

However, social media can also create risks to adults, young people, vulnerable adults and Parish / Youth Ministry personnel. Safeguarding, privacy, dignity and the wellbeing of all involved must therefore remain at the heart of social media use.

This policy should be read alongside the Diocese's safeguarding procedures, communications policy, mobile phone and photography guidance, and any other relevant diocesan policies. It is intended to be reviewed at least annually and sooner where significant changes in platforms, technology, safeguarding guidance or legislation occur.

2.0 Guidelines for Parishes / Youth Ministry Using Social Media with Young People (Under 18s)

Written parent / guardian consent must be obtained where the Diocese, Parish or Youth Ministry intends to communicate with, photograph, record or otherwise feature a person under 18 through social media, subject to the Diocese's current safeguarding and photography procedures.

Do not use disappearing-message functions for safeguarding-related communication. Communications should be capable of being retained where required by safeguarding or record-management procedures.

Official accounts must be used for Parish / Youth Ministry purposes and should not operate as an individual employee or volunteer's personal account.

One-to-one communication with young people or vulnerable adults should be avoided. Where communication is necessary, it should be visible, accountable and conducted through approved channels, with appropriate adults included where practicable.

Where a communication cannot appropriately be dealt with publicly or through the normal group channel, contact the parent/guardian where appropriate and/or the Director of Safeguarding. In an emergency, contact the appropriate authorities in accordance with safeguarding procedures.

Personnel should not use personal social-media accounts to privately message, follow, friend or otherwise connect with young people or vulnerable adults because of their Archdiocesan role, unless an existing relationship outside that role is clearly established and the contact is appropriate and consistent with safeguarding requirements.

2.1 Facebook / Messenger

Any Parish / Youth Ministry Facebook account must be used for Parish / Youth Ministry purposes only. Messages and other safeguarding-relevant communications should be retained in accordance with the Diocese's record-management requirements.

Messenger must not be used for private one-to-one communication with young people or vulnerable adults. Where a response to a private message is needed, respond through an appropriate public or accountable channel where possible.

The account should not be used after 11pm. Communication must remain appropriate, professional and consistent with this policy.

2.2 X and Similar Platforms (including Bluesky)

Official accounts must be managed only by appointed administrators. Posts must reflect the ethos and guiding principles of the Diocese and must not be used to promote an individual's personal interests.

Posts should be retained in accordance with the Diocese's record-management requirements. Young people may follow an official account, but Parish / Youth Ministry accounts should not follow young people back.

Direct messaging with young people or vulnerable adults must not be used. The account should not be used after 11pm.

2.3 Instagram

Instagram accounts must be managed by appointed administrators. Images and videos must be appropriate, and required parental/guardian consent must be obtained before a child is photographed or featured.

Where possible, use group photographs rather than individual photographs and avoid publishing a child's full name with an image. Remember that images can be copied, altered and redistributed outside the control of the Diocese.

Images and videos used for official communications should be retained in an appropriate diocesan or parish folder in line with record-management requirements.

Young people may follow official accounts, but Parish / Youth Ministry accounts should not follow young people back. Replies to comments should be limited to appropriate, factual responses, such as event queries.

2.4 Snapchat

The use of Snapchat by Diocesan Groups, Parishes or Youth Ministry Groups is not permitted. Its ephemeral design and disappearing content make accountable safeguarding, retention and review difficult.

2.5 WhatsApp

WhatsApp may be used for group communication where it supports the activity and where the relevant safeguarding and consent requirements are met. The platform's current terms and age requirements should be checked before use; the policy should not rely on a fixed age statement that may become outdated.

Written parent / guardian permission should be obtained before adding under-18s to a youth-group WhatsApp group. Where a group includes both adults and under-18s, separate groups should be considered where appropriate.

At least two Garda-vetted adults should be members of any WhatsApp group involving under-18s. Only appropriately vetted leaders should participate in such groups.

When a young person leaves a youth group, they should be removed from the group where appropriate and in accordance with the group's records and privacy procedures.

Adding someone to a WhatsApp group can disclose their mobile number to other members. Leaders should therefore consider privacy before creating or adding people to groups.

Do not use disappearing messages for safeguarding-related communication. Where appropriate and lawful, retain relevant group communications in accordance with diocesan record-management requirements.

2.6 TikTok

Any TikTok account must be managed by the appointed Parish / Youth Ministry administrator and used only for approved purposes.

Videos must be appropriate, consistent with the ethos and guiding principles of the Diocese and supported by the required consent. Do not use the account to showcase personal interests.

Young people may follow official Parish / Youth Ministry accounts, but official accounts should not follow young people back. Engagement with comments should be limited to appropriate, factual responses, such as event queries.

The account should not be used after 11pm.

2.7 YouTube

Parishes / Youth Ministry using YouTube must do so responsibly and select the most appropriate audience and privacy settings for each upload.

Before publishing, check that all people featured have the required consent, that copyright and privacy requirements are met, and that the content is suitable for children where children may access it.

3.0 Artificial Intelligence (AI): Best Practice

AI includes generative AI tools such as chatbots, image generators, transcription tools, translation tools and other systems that create, transform, summarise or analyse content. AI can support administration and communications, but it must never replace safeguarding judgement, human oversight or the responsibilities of staff and volunteers.

3.1 Approved and appropriate uses

AI may be used for low-risk tasks such as brainstorming, drafting generic communications, improving readability, producing non-personalised ideas, or assisting with formatting, provided the final content is checked by a person before use.

3.2 Protect personal and safeguarding information

Do not enter personal data, safeguarding records, disclosures, photographs of children, contact details, health information, confidential pastoral information, passwords, internal incident information or other sensitive information into a public or unapproved AI tool. Publicly available personal information can still be personal data. Where AI processing involves personal data, the Diocese must consider lawful basis, transparency, data

minimisation, security and whether a Data Protection Impact Assessment or other data-protection assessment is required.

3.3 Human checking is mandatory

AI-generated text, images, audio or video must be checked by an appropriately responsible person before publication or use. Check accuracy, context, tone, safeguarding implications, factual claims, names, dates, quotations, scripture references and any statements presented as fact. AI can produce plausible but incorrect or misleading material.

3.4 Children and vulnerable people

Do not use AI to assess, rank, profile, predict or make decisions about a child or vulnerable adult. Do not use AI to create or alter an image of a child in a way that could misrepresent the child, expose them to risk or undermine their dignity. Never use AI to generate sexualised, humiliating or exploitative material involving children or young people.

3.5 AI-generated images, audio and video

Do not create or publish realistic AI-generated or AI-manipulated content that could reasonably be mistaken for an authentic recording of a person or event without appropriate review, permission and clear disclosure. Particular care is required with deepfakes and synthetic images involving children or identifiable individuals.

3.6 Transparency and labelling

Where AI is used to create or substantially alter content, consider whether disclosure or labelling is required by law, platform rules or Archdiocesan practice. From 2 August 2026, relevant transparency obligations under the EU AI Act apply, including requirements concerning certain AI interactions and AI-generated or manipulated content.

3.7 Copyright, accuracy and faith content

Do not assume that AI-generated material is accurate, original or free of copyright restrictions. Check sources where factual claims are important. Scripture, Church teaching, safeguarding guidance, legal information and official diocesan statements must be checked against authoritative sources and must not be invented or altered by an AI tool.

3.8 Approved tools and accountability

Use only AI services approved by the Diocese where an organisational account, subscription or processing of organisational information is involved. Keep a clear human decision-maker for every published AI-assisted communication. If an AI tool produces harmful, discriminatory, sexual, misleading or otherwise inappropriate content, stop using the output and report the concern through the appropriate safeguarding, data-protection or management route.

3.9 A simple rule

If you would not put the information, photograph or message into a public social-media post, do not put it into a public AI tool. When in doubt, do not upload it: ask the relevant safeguarding or data-protection contact first.

AI decision test

Before using an AI tool, ask: (1) Is the information safe to share? (2) Is the use necessary and appropriate? (3) Have I kept a human in control? (4) Have I checked the output? (5) Does anyone need to know that AI was used?

4.0 General Social Media Guidelines

Be responsible. When in doubt about the content, image or tone of a post, leave it out. Social-media language may be informal, but official communications should remain respectful, professional and appropriate.

Protect privacy. Use appropriate privacy and moderation settings. Monitor official accounts regularly and remove or restrict content that breaches site rules, safeguarding requirements or diocesan standards, while retaining evidence where a safeguarding or legal concern requires it.

Do not permit obscene, harassing, threatening, offensive, discriminatory, derogatory or defamatory content. Do not publish material that could put a child, vulnerable adult, employee, volunteer or member of the public at risk.

Each official social-media account should have at least two appropriately authorised administrators to support continuity, rapid response and oversight.

Comply with copyright, licensing, privacy and data-protection requirements. Obtain permission before using third-party photographs, music, video or other protected material unless a lawful exception or licence applies.

Use photographs responsibly. Where possible, disable tagging of children and limit visitor posting where the platform permits. Follow the Diocese's mobile-phone and photography guidance.

Personal accounts are not official Archdiocesan channels. Employees and volunteers should nevertheless avoid conduct that could undermine safeguarding, confidentiality, professional boundaries or the reputation of the Diocese.

Keep records of significant safeguarding-related communications, complaints, incidents and decisions in accordance with diocesan procedures. Do not delete potentially relevant evidence simply because a post or message is no longer publicly visible.

Escalate safeguarding concerns promptly through the Diocese's safeguarding procedures. Social media is never a substitute for reporting a concern through the appropriate safeguarding or statutory channel.

This policy will be reviewed at least annually and updated sooner where significant changes occur in social-media platforms, AI technology, safeguarding guidance or legislation.

5.0 Useful Websites, Relevant Legislation and Diocesan Policies

Relevant diocesan policies and guidance include: Guidance on the Use of CCTV and Webcams; Communications Policy; Mobile Phone and Photography Guidance; Guidelines for Use of Social Media to Broadcast Mass and Prayers; and the Archdiocesan safeguarding policies and procedures.

Useful websites include: Diocese of Killaloe's safeguarding resources; Data Protection Commission (dataprotection.ie); Coimisiún na Meán (cnam.ie); Webwise (webwise.ie); FraudSMART (fraudsmart.ie); An Garda Síochána Cyber Crime resources (garda.ie); Take It Down (takeitdown.ncmec.org); and Hotline.ie.

Key legislation and regulatory frameworks to keep under review:

- Children First Act 2015 and Children First: National Guidance for the Protection and Welfare of Children (2017), including the online-safety addendum.
- Criminal Law (Sexual Offences) Act 2017, including offences relating to the sexual exploitation of children and use of information and communication technology to facilitate sexual exploitation.
- Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR).
- Harassment, Harmful Communications and Related Offences Act 2020, including offences relating to harassment, intimate images and threatening or grossly offensive communications.
- Online Safety and Media Regulation Act 2022 and the Online Safety Code overseen by Coimisiún na Meán.
- Digital Services Act 2024, which gives effect in Ireland to the EU Digital Services Act (Regulation (EU) 2022/2065).
- Regulation (EU) 2024/1689 (EU Artificial Intelligence Act). The AI Act entered into force in 2024 and its provisions apply progressively; AI-literacy obligations began applying from 2 February 2025 and the main application date was 2 August 2026, subject to the Act's phased provisions.

Legislation and guidance can change. The Director of Safeguarding / relevant diocesan lead should verify current requirements when this policy is reviewed.

Document control

Owner: Diocese of Killaloe Safeguarding | Review cycle: At least annually | Current version: October 2026