

SOCIAL MEDIA POLICY TEMPLATE

For Religious Organizations

A practical policy template for clergy, staff, volunteers, ministries, official accounts, youth communication, confidentiality, fundraising, and online conduct.

Organization: [Organization Name]

Version: [Version Number]

Effective Date: [Effective Date]

Owner: [Department or Role]

Contact: [Contact Email or Channel]

Important note

This template is a starting point and should be reviewed by legal counsel, HR, communications, safe environment, privacy, youth protection, and ministry leadership before use. It is not legal advice.

Table of Contents

1. Purpose
2. Who this policy applies to
3. Platforms covered by this policy
4. Personal accounts vs. official organization accounts
5. Official voice and personal opinions
6. Respectful communication
7. Confidential information
8. Youth, minors, and vulnerable adults
9. Photos and videos of minors, members, and events
10. Official accounts and account access
11. Boundaries for clergy, staff, and ministry leaders
12. Donors, fundraising, and financial matters
13. Public comments and moderation
14. Crisis, safety, and sensitive situations
15. Copyright, trademarks, and third-party content
16. Reviews, endorsements, and public recommendations
17. Use of AI-generated content
18. Employee and volunteer rights are respected
19. Reporting concerns
20. When to ask for help
21. Policy violations
22. Related policies
23. Acknowledgment

Policy Summary

- Use official accounts only when authorized and follow [Organization Name] approval, security, and account access procedures.
- Keep personal opinions separate from official organization statements.
- Protect confidential information, including pastoral care, counseling, donor, member, youth, student, employee, and safe environment information.
- Maintain appropriate boundaries with minors, vulnerable adults, members, students, donors, and volunteers.
- Do not post photos or videos of minors, members, or events unless policy allows it and required consent is in place.
- Escalate media inquiries, crisis matters, legal issues, safety concerns, fundraising claims, and sensitive community issues to [Department or Role].

Policy note

Religious organizations should adapt this policy to their denomination, governance structure, school or youth programs, safe environment rules, donor privacy obligations, and applicable state or local laws.

1. Purpose

[Organization Name] recognizes that social media can be a meaningful tool for ministry, communication, outreach, education, fundraising, event promotion, and community building.

This policy explains how clergy, staff, volunteers, ministry leaders, teachers, coaches, contractors, and authorized representatives should use social media when their activity may relate to [Organization Name], its ministries, members, students, youth, families, donors, employees, volunteers, facilities, events, beliefs, or reputation.

The goal of this policy is not to control every personal post. The goal is to protect the people we serve, maintain appropriate boundaries, preserve trust, communicate respectfully, protect confidential information, and ensure that official online communication reflects the mission and values of [Organization Name].

2. Who this policy applies to

This policy applies to all individuals serving, working, volunteering, or representing [Organization Name], including clergy, ministers, pastors, religious leaders, employees, teachers, youth ministry leaders, coaches, volunteers, contractors, communications staff, program leaders, ministry coordinators, and anyone authorized to manage or post from an official account.

This policy applies to personal social media use when posts relate to [Organization Name], its ministries, members, students, youth, families, donors, employees, volunteers, events, facilities, services, or official activities. It also applies to official accounts for [Organization Name], affiliated schools, parishes, congregations, ministries, youth groups, departments, programs, events, and community initiatives.

3. Platforms covered by this policy

This policy applies to social media platforms, messaging apps, livestreaming platforms, online communities, blogs, forums, review sites, video platforms, private groups, and public comment sections.

Examples include Facebook, Instagram, TikTok, X, LinkedIn, YouTube, Snapchat, Threads, Reddit, Discord, WhatsApp, GroupMe, Slack, Microsoft Teams, blogs, forums, review sites, private groups, livestream platforms, and any future platform where users post, comment, share, message, stream, or upload content.

Private accounts, disappearing messages, restricted groups, or friends-only settings do not guarantee privacy. Screenshots, reposts, forwarded messages, recordings, and archives can still exist after the original post is deleted.

4. Personal accounts vs. official organization accounts

Individuals may use personal social media accounts for personal expression. However, they should make clear when they are speaking for themselves and not for [Organization Name].

Only authorized individuals may create, manage, or post from official [Organization Name] social media accounts. No one may create accounts, pages, groups, usernames, or profiles that appear to represent [Organization Name], a congregation, parish, school, ministry, youth group, department, event, or program unless approved by [Department or Role].

Official accounts should be created, owned, and managed according to [Organization Name] procedures. Account access should not be tied only to one individual personal email, phone number, or personal profile.

5. Official voice and personal opinions

Unless authorized, individuals may not present personal opinions as official statements from [Organization Name]. They should avoid language such as "[Organization Name] believes," "our official position is," "we are announcing," or "on behalf of [Organization Name]" unless approved.

When discussing matters related to [Organization Name], individuals should make clear when they are sharing a personal view. Examples include: "I serve with [Organization Name], but these views are my own," or "I am not speaking on behalf of [Organization Name]."

Media inquiries, legal questions, public complaints, sensitive community issues, crisis matters, and questions about official positions should be referred to [Department or Role].

6. Respectful communication

All social media activity connected to [Organization Name] should reflect respect, dignity, honesty, and care for others.

Individuals should not use social media to harass, threaten, bully, shame, intimidate, demean, or target members, students, youth, families, donors, coworkers, volunteers, clergy, community members, or members of the public.

This policy applies even when posts are made from personal accounts or outside working or volunteer hours if the conduct affects [Organization Name], its ministries, the people it serves, or the community.

- Harassment, threats, bullying, doxxing, sexual harassment, discriminatory comments, mocking vulnerable people, posting private information about others, encouraging harassment by others, and retaliation for raising a concern are prohibited.

7. Confidential information

Individuals may not post, share, upload, livestream, screenshot, forward, or disclose confidential or private information learned through their role with [Organization Name].

If information is not public, do not make it public. When in doubt, do not post. Ask [Department or Role] first.

- Pastoral care conversations, counseling information, private prayer requests, donor information, member records, student or youth records, volunteer records, employee records, safe environment reports, legal matters, financial information, security procedures, internal emails or messages, personnel matters, private family situations, medical information, non-public announcements, and sensitive ministry issues.

8. Youth, minors, and vulnerable adults

[Organization Name] is committed to protecting minors and vulnerable adults. Individuals may not use social media, messaging apps, private groups, or direct messages in ways that violate safe environment, youth protection, school, ministry, or child safety policies.

Youth ministry, school, athletic, and program communication should happen through approved channels, official accounts, parent-approved communication tools, or other systems approved by [Organization Name].

- Do not privately message minors from personal accounts unless specifically allowed by policy.
- Do not use disappearing messages for youth or ministry communication.
- Do not add current minors as friends or followers on personal accounts.
- Do not create unofficial youth groups without approval.
- Do not post content that embarrasses, exposes, or singles out a minor.

9. Photos and videos of minors, members, and events

Photos and videos can be valuable for sharing the life of a religious community, but they must be handled carefully.

Individuals may not post photos, videos, livestreams, or recordings of minors, members, students, families, volunteers, or participants unless allowed by [Organization Name] policy and supported by required consent.

Before posting images or videos, confirm that the account is authorized, required consent or media release is on file, the post follows communications guidelines, the image does not reveal confidential information, and the content reflects the values and mission of [Organization Name].

- Avoid posting photos or videos from counseling settings, private pastoral care meetings, restrooms, locker rooms, health offices, classrooms where privacy may be affected, sensitive ministry settings, safe environment incidents, medical emergencies, discipline situations, and private family matters.

10. Official accounts and account access

Only authorized individuals may manage official [Organization Name] accounts. Official accounts may include accounts for the organization, parishes or congregations, schools, youth ministries, children ministries, outreach programs, fundraising campaigns, events, departments, service projects, volunteer groups, and community initiatives.

Individuals with official account access must use approved login methods, multi-factor authentication where required, brand and communications guidelines, approved images and copy, approval workflows, and copyright and trademark rules.

When a person leaves [Organization Name] or changes roles, access to official accounts must be removed promptly.

- Protect credentials and never share passwords outside approved systems.
- Protect confidential information.
- Avoid personal opinions from official accounts.
- Escalate sensitive issues quickly.
- Report access issues immediately.

11. Boundaries for clergy, staff, and ministry leaders

Clergy, staff, ministry leaders, teachers, coaches, and volunteers may hold positions of trust. Their online conduct may be more closely associated with [Organization Name].

Leaders should model good judgment and ask [Department or Role] before posting about sensitive topics.

- Do not use personal social media to pressure members, students, youth, donors, or volunteers.
- Do not discuss private pastoral, personnel, school, or ministry matters online.
- Do not post about discipline, counseling, family disputes, safe environment concerns, investigations, or personnel issues.
- Do not retaliate against someone for reporting a concern.
- Do not use social media to shame, pressure, or publicly correct individuals.

12. Donors, fundraising, and financial matters

Employees, clergy, volunteers, and representatives should handle fundraising and donor-related communication carefully.

Individuals may not post private donor information, donation amounts, giving history, financial records, or confidential fundraising discussions.

Fundraising posts, campaigns, donation links, sponsorships, contests, raffles, giveaways, and appeals should be approved by [Department or Role] before publication.

- Do not make false, misleading, exaggerated, or unauthorized claims about donation use, program impact, tax deductibility, matching gifts, fundraising goals, beneficiary stories, sponsorships, emergency relief efforts, financial needs, or campaign deadlines.

13. Public comments and moderation

Official accounts should encourage respectful, constructive conversation. [Organization Name] may moderate comments to protect the community, maintain respectful dialogue, and prevent harm.

Moderation should be consistent, fair, and based on behavior rather than disagreement alone.

- Comments may be removed, hidden, reported, or escalated when they include threats, harassment, hate speech, personal attacks, obscenity, spam, scams, impersonation, confidential information, private information about others, content that endangers minors or vulnerable adults, or content that disrupts ministry, school, safety, or operations.

14. Crisis, safety, and sensitive situations

Individuals may not post on behalf of [Organization Name] about emergencies, accidents, misconduct allegations, abuse reports, investigations, legal matters, security threats, deaths, injuries, violence, or crisis situations unless authorized.

Follow [Organization Name] crisis communication procedures and refer questions to [Department or Role].

- Do not share names of individuals involved, investigation details, police or legal matters, internal response plans, security procedures, medical information, photos or videos from crisis scenes, rumors, unverified information, or private family or victim information.

15. Copyright, trademarks, and third-party content

Individuals should not post content that belongs to someone else unless they have permission or the content is approved for use.

Individuals may not misuse [Organization Name] logos, names, symbols, ministry marks, school marks, slogans, event names, or brand assets.

- Photos, videos, music, logos, artwork, sermon clips from outside sources, religious education materials, curriculum materials, presentations, livestream recordings, written reflections, donor or partner content, student or youth work, and internal documents should be used only when permitted.

16. Reviews, endorsements, and public recommendations

Individuals may not post fake reviews, misleading reviews, or anonymous endorsements of [Organization Name], its schools, ministries, programs, events, or affiliated services.

If individuals promote or endorse [Organization Name] programs, services, events, or initiatives online, they should disclose their connection when appropriate.

Individuals may not offer unauthorized rewards, gifts, incentives, discounts, special treatment, or benefits in exchange for reviews, endorsements, testimonials, or public support.

17. Use of AI-generated content

Individuals should be careful when using AI tools to create social media content related to [Organization Name].

Do not enter confidential information, pastoral care details, donor information, member information, student information, youth information, personnel information, legal matters, or internal documents into unapproved AI tools.

AI-generated content for official accounts must follow review and approval procedures. Individuals are responsible for checking AI-generated content for accuracy, privacy risk, bias, copyright concerns, tone, and alignment with [Organization Name] values before posting.

18. Employee and volunteer rights are respected

Nothing in this policy is intended to prevent employees from discussing wages, hours, working conditions, workplace safety, benefits, or other rights protected by law.

Employees may have the right to discuss workplace concerns with coworkers, government agencies, labor organizations, or others.

Employees should still avoid sharing confidential member information, donor information, student information, private personnel records, safe environment information, or security-sensitive information when discussing workplace concerns.

19. Reporting concerns

Individuals should report social media activity that may violate this policy or create risk for [Organization Name].

Reports can be made to [Department or Role], [HR Contact], [Safe Environment Contact], [Communications Contact], [Legal Contact], [Security Contact], or [Anonymous Reporting Channel if applicable].

[Organization Name] prohibits retaliation against individuals who report concerns in good faith.

- Unsafe communication with minors, unauthorized photos or videos of minors, disclosure of confidential information, harassment or threats, fake organization accounts, impersonation, misuse of logos or names, security risks, unauthorized media comments, misleading fundraising claims, inappropriate comments from official accounts, and photos or videos from restricted areas should be reported.

20. When to ask for help

Ask [Department or Role] before posting if content involves minors, vulnerable adults, photos or videos from organization activities, pastoral care or counseling, confidential information, donor information, school or youth ministry matters, safe environment concerns, legal issues, media requests, public complaints, fundraising claims, crisis situations, official organization positions, organization logos or branding, or anything that could be mistaken for an official statement.

Questions should be directed to [Contact Email or Channel].

21. Policy violations

Violations of this policy may result in corrective action, loss of volunteer privileges, removal of account access, disciplinary action, termination, or other action depending on the facts, applicable law, and [Organization Name] policy.

[Organization Name] will review each situation based on the facts, applicable law, organizational policy, and impact on the community.

- Sharing confidential information, posting unauthorized photos or videos of minors, unsafe or inappropriate communication with minors, speaking for [Organization Name] without authorization, harassing members or staff online, misusing official accounts, sharing account passwords, posting unauthorized crisis information, misusing organization logos or trademarks, making misleading fundraising claims, and retaliating against protected activity or good-faith reporting.

22. Related policies

Individuals should also review and follow related [Organization Name] policies.

- Code of Conduct
- Employee Handbook
- Volunteer Handbook
- Safe Environment Policy
- Child and Youth Protection Policy
- Confidentiality Policy
- Media Relations Policy
- Fundraising Policy
- Photography and Video Consent Policy
- Acceptable Use of Technology Policy
- Anti-Harassment and Anti-Discrimination Policy
- Records Retention Policy
- Crisis Communications Policy
- AI Use Policy
- Copyright and Trademark Policy
- Disciplinary Action Policy

23. Acknowledgment

I acknowledge that I have received and reviewed the [Organization Name] Social Media Policy. I understand that I am responsible for following this policy when using social media in ways that relate to [Organization Name], its ministries, members, students, youth, families, donors, employees, volunteers, facilities, events, or reputation.

I understand that this policy does not prevent me from exercising rights protected by applicable law.

Name: _____

Role: _____

Signature: _____

Date: _____