SOCIAL MEDIA POLICY TEMPLATE

For Nonprofit Organizations

A practical policy template for staff, volunteers, board members, official accounts, fundraising, donor privacy, client dignity, public engagement, 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, fundraising, privacy, and program leadership before use. It is not legal advice.

Table of Contents

1. Purpose

[Organization Name] recognizes that social media can be a valuable tool for advancing our mission, communicating with supporters, serving our community, sharing impact stories, recruiting volunteers, fundraising, and building public trust.

This policy explains how employees, volunteers, board members, contractors, interns, and authorized representatives should use social media when their activity may relate to [Organization Name], its mission, programs, donors, clients, beneficiaries, volunteers, partners, employees, events, campaigns, or reputation.

The goal is not to control every personal post. The goal is to protect the people we serve, respect donor and client privacy, communicate accurately, maintain trust, 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 working with, volunteering for, serving, or representing [Organization Name], including full-time, part-time, temporary, volunteer, board, committee, intern, contractor, consultant, program, fundraising, communications, event, and community outreach roles.

This policy applies to personal social media use when posts relate to [Organization Name], its mission, programs, donors, clients, beneficiaries, volunteers, staff, events, campaigns, partners, or public reputation. It also applies to official accounts used for programs, fundraising campaigns, events, chapters, committees, volunteer groups, or 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, fundraising platforms, and public comment sections.

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.

- Facebook, Instagram, TikTok, X, LinkedIn, YouTube, Threads, Reddit, Discord, WhatsApp, GroupMe, Slack, Microsoft Teams, blogs, forums, review sites, livestream platforms, private groups, and future platforms.

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 program, chapter, local office, campaign, volunteer group, event, or initiative unless approved by [Department or Role]. Official account access should not be tied only to one person’s personal email, phone number, or personal social media profile.

5. Official voice and personal opinions

Unless authorized, individuals may not present personal opinions as official statements from [Organization Name]. When discussing matters related to [Organization Name], individuals should make clear when they are sharing a personal view.

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

- Use clarifying statements such as: "I work with [Organization Name], but these views are my own," or "I volunteer with [Organization Name], but I am not speaking on behalf of the organization."

6. Mission-aligned communication

Social media activity connected to [Organization Name] should support the organization’s mission, values, and public trust. Official accounts should not be used for personal opinions, political arguments, private disputes, personal fundraising unrelated to [Organization Name], or content that conflicts with the organization’s mission and policies.

- Official communication should be accurate, respectful, clear, mission-focused, inclusive, helpful, professional, transparent, and consistent with approved messaging.

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.

- Client, beneficiary, donor, volunteer, employee, and board information; internal investigations; legal matters; financial information; grant applications or reports not intended for public release; internal emails or messages; program data; case files; intake information; medical, housing, family, or financial details about people served; security procedures; and non-public announcements.

8. Privacy of clients, beneficiaries, and people served

[Organization Name] is committed to protecting the dignity and privacy of the people it serves. Individuals may not post stories, photos, videos, names, personal details, or identifying information about clients, beneficiaries, program participants, families, or community members unless allowed by policy and supported by required consent.

Even if a name is not used, a post may still violate privacy if the person can reasonably be identified. Individuals should avoid language or images that exploit, shame, stereotype, or reduce people to their hardships.

9. Photos, videos, and storytelling

Photos, videos, and personal stories can help show the impact of [Organization Name], but they must be handled carefully. Before posting images, videos, testimonials, or stories, confirm that required consent or release forms are complete, the content protects dignity and privacy, the story is accurate, and the content is approved by [Department or Role] when required.

Avoid posting photos or videos from private service settings, counseling or case management meetings, medical or crisis situations, domestic violence or shelter-related locations, youth programs without consent, or any location where safety or confidentiality may be compromised.

10. Donor privacy and fundraising ethics

Individuals must protect donor privacy and handle fundraising communication responsibly. Do not post private donor information, including donation amounts, giving history, contact information, anonymous donor identities, payment information, internal donor notes, private donor conversations, unapproved donor testimonials, corporate partner terms, or grant details not intended for public release.

Fundraising posts, donation links, sponsorships, contests, raffles, giveaways, emergency appeals, and campaign claims should be approved by [Department or Role] before publication. All fundraising communication should be accurate, respectful, transparent, and aligned with [Organization Name] policies.

11. Volunteers, board members, and ambassadors

Volunteers, board members, ambassadors, and community advocates can help expand the reach of [Organization Name]. They should share approved public information, avoid confidential information, avoid speaking as official representatives unless authorized, use approved campaign language when available, respect privacy, disclose their relationship when appropriate, and refer media or public complaints to [Department or Role].

Board members and high-visibility representatives should use extra care because their posts may be associated with [Organization Name] even when posted from personal accounts.

12. Respectful public engagement

All social media activity connected to [Organization Name] should reflect respect, dignity, and care for others. Individuals should not use social media to harass, threaten, bully, shame, intimidate, discriminate against, dox, or target clients, beneficiaries, donors, volunteers, employees, partners, 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 work, the people it serves, or the community.

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. Official accounts should include clear community guidelines where appropriate.

- 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, misinformation related to official matters, or content that endangers people or disrupts programs.

14. Political activity and advocacy

Some nonprofits engage in advocacy, public education, or policy work. Others may be limited in the political activity they can conduct. Individuals may not use official [Organization Name] accounts for political endorsements, campaign activity, lobbying, ballot issues, or public policy statements unless approved by [Department or Role] and compliant with applicable law and organizational rules.

Employees, volunteers, and board members may engage in personal civic or political activity, but they should not imply that [Organization Name] endorses their personal views unless authorized.

15. Crisis, emergency, and sensitive situations

Individuals may not post on behalf of [Organization Name] about emergencies, investigations, misconduct allegations, deaths, injuries, abuse reports, data incidents, legal matters, security threats, 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, legal matters, internal response plans, security procedures, medical information, photos or videos from crisis scenes, rumors or unverified information, private family or victim information, or internal communications.

16. Official account access and security

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

- Use approved login methods and multi-factor authentication where required; protect credentials; follow brand and communications guidelines; use approved content; respect copyright and trademark rules; protect confidential information; follow approval workflows; avoid personal opinions from official accounts; escalate sensitive issues quickly; report access issues immediately; and never share passwords outside approved systems.

17. 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, slogans, campaign marks, event names, program names, or brand assets.

- Photos, videos, music, logos, artwork, testimonials, donor content, partner content, client stories, volunteer content, program materials, training materials, grant materials, internal documents, and unreviewed AI-generated content.

18. Reviews, endorsements, and testimonials

Individuals may not post fake reviews, misleading reviews, or anonymous endorsements of [Organization Name], its programs, events, campaigns, services, or partners. If individuals promote or endorse [Organization Name] programs, campaigns, services, or initiatives online, they should disclose their connection when appropriate.

Testimonials, success stories, impact stories, and partner quotes should be approved by [Department or Role] before publication.

19. 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, donor information, client information, beneficiary information, employee information, volunteer information, financial information, grant 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.

20. 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 client information, donor information, private personnel records, grant information, security-sensitive information, or legally protected information when discussing workplace concerns.

Policy note

This section should be reviewed by counsel to make sure the final policy complies with labor and employment laws in all applicable jurisdictions.

21. 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], [Volunteer Manager], [Communications Contact], [Legal Contact], [Security Contact], or [Anonymous Reporting Channel if applicable]. [Organization Name] prohibits retaliation against individuals who report concerns in good faith.

- Examples include disclosure of confidential information, unauthorized photos or videos, harassment or threats, fake organization accounts, impersonation, misuse of logos or organization names, security risks, unauthorized media comments, misleading fundraising claims, inappropriate comments from official accounts, privacy concerns, and account access issues.

22. When to ask for help

Ask [Department or Role] before posting if content involves clients or beneficiaries, minors or vulnerable people, photos or videos from programs or events, donor information, fundraising claims, confidential information, legal issues, media requests, public complaints, grant or program data, crisis situations, official organization positions, organization logos or branding, partner announcements, political or advocacy content, or anything that could be mistaken for an official statement.

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

23. 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.

- Examples include sharing confidential information, posting unauthorized photos or videos, sharing donor information, speaking for [Organization Name] without authorization, harassment, misusing official accounts, sharing account passwords, posting unauthorized crisis information, misusing organization logos or trademarks, making misleading fundraising claims, and retaliation.

24. Related policies

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

- Code of Conduct, Employee Handbook, Volunteer Handbook, Confidentiality Policy, Donor Privacy Policy, Client Privacy Policy, Fundraising Policy, Media Relations 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, and Disciplinary Action Policy.

25. 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 mission, programs, clients, beneficiaries, donors, employees, volunteers, partners, events, campaigns, or reputation.

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

Name: _____

Role: _____

Signature: _____

Date: _____