

A FREE UNCOM MEDIA RESOURCE



Social Media Policy & Procedures **Guide**

For Businesses, Nonprofits & Organizations of Every Size

CLARITY • CONSISTENCY • TRUST

A Note Before You Start

Somewhere in your organization right now, someone has the login to your social media accounts. Maybe it is a marketing coordinator. Maybe it is the founder, still posting from a personal phone. Maybe it is three different people who each think someone else is in charge of what happens if a post goes wrong.

That gap, the one between "someone probably has this handled" and an actual, written plan, is where most social media problems start. Not with a bad actor. With a good team that never got around to writing down who owns what, what gets said, and what happens on the day something goes sideways.

Social media is no longer a side project you hand to whoever is youngest or most online. For most organizations today, it is a primary channel for reputation, recruiting, customer trust, and revenue, all running in public, in real time, often faster than leadership can react.

WHY THIS MATTERS

A policy is not a document you write to restrict people. It is a shared understanding, written down before you need it, so your team can move quickly and confidently on a normal Tuesday and stay level-headed on the day it isn't.

This guide is intentionally general. It is built to apply whether you run a five-person startup, a regional healthcare system, a manufacturing company, a law firm, or a national nonprofit. Adapt it to your structure, your industry, and your risk tolerance. Use what fits, and set aside what doesn't.

We built this at UNCOM Media because we have sat across the table from leaders in the middle of a moment that could have been meaningfully softened by a plan written months earlier. Preparation is cheap. Improvising in public is not.

Read through it, adapt it to your organization, and put it to work. And if you would like help building the complete version of this, tailored to your team, your industry, and your specific risks, we would love to talk.

With clarity,

The UNCOM Media Team

Table of Contents

01	Why Every Organization Needs a Social Media Policy	4
02	Roles & Responsibilities	5
03	Choosing the Right Platforms for Your Organization	6
04	Your Team & Account Inventory (Fillable)	7
05	Content Guidelines & Voice	9
06	Approval & Posting Workflow	10
07	Protecting People: Employees, Customers & Minors	11
08	Managing Comments & Public Interaction	13
09	When Things Go Wrong: A Basic Crisis Protocol	14
10	Account Security Basics	15
11	Copyright & Legal Basics	16
12	Sample Policy Statement & Staff Agreement	17
13	Quick-Start Checklist	18

Why Every Organization Needs a Social Media Policy

Every organization with a social account is, whether it planned to be or not, a publisher. Your posts, your comment sections, and your employees' personal profiles are all part of how customers, partners, investors, and future hires form their opinion of you, often before they ever speak to a human being.

That reach cuts both ways. A single well-timed post can build trust and drive real business results. A single careless one, posted without a second set of eyes, can undo years of goodwill in an afternoon. The difference between those two outcomes is rarely talent. It's usually just whether a plan existed.

What changes as you grow

A one-person team can often get away with informal ownership. Once more than one person can post, once your brand shows up across multiple platforms, or once a founder or executive has a public following of their own, informal ownership stops being efficient and starts being a liability. Multiple hands touching the same brand, without shared rules, is how tone drifts, mistakes slip through, and nobody is quite sure who is supposed to respond when something goes wrong.

WHY THIS MATTERS

A policy exists to give your team a shared, tested framework for both everyday content and the rare high-stakes moment, so nobody is building the plan from scratch under pressure, in public, while the clock is running.

What a policy actually does for you

- **It protects your reputation.** Across every account, every platform, and every person who represents your brand.
- **It protects your leadership team.** By creating a documented escalation path instead of ad hoc decision-making under pressure.
- **It creates consistency.** So your brand sounds like one organization, no matter how many hands are involved.
- **It gives you a real plan for hard days.** Including the ones with genuine legal, financial, or reputational consequences.

This guide walks through all of it, built to scale up or down depending on the size and shape of your organization.

Roles & Responsibilities

Social media should sit within a real function of your organization, with a named owner, defined production roles, and a clear, short path to executive and legal sign-off when something is sensitive.

Recommended structure

Role	Who it usually is	What they do
Director of Communications / Marketing	Senior staff member, often reporting to the CEO or President	Owns brand strategy and governance, manages the team, sets the content calendar, is the default spokesperson for routine matters
Social Media Manager(s) & Content Producers	Staff specialists in social, video, design, or copy	Executes day-to-day content, scheduling, and comment moderation across primary accounts
Team, Department, or Location Leads	Staff or manager at each office, franchise, or business unit	Manage local content within brand guidelines, report to the central communications team
Customer Experience / Community Lead	Staff member overseeing digital customer engagement	Owns comment and message response across channels, coordinates with the broader team
Executive Leadership (CEO / President)	Final approving authority	Sign-off on sensitive, brand-defining, or crisis-related content, in coordination with legal and the board when needed

RIGHT-SIZED ADVICE

Informal ownership is a real liability, even at a small organization. Every role above should exist somewhere in writing, not just in practice, with a clear line up to leadership. A solo founder can fill several rows on this table. What matters is that each function has a name attached.

Public-facing leaders and personal platforms

Founders, executives, and other public-facing employees should have a direct, respectful working relationship with the communications team regarding their personal platforms, since these are widely perceived as extensions of the brand whether or not that was ever formally decided. This should be a collaborative relationship built on shared understanding, not a compliance exercise.

Setting expectations up front

- Formalize every role, including any team or location lead, in writing, and revisit it at least annually
- Give every team and platform the same governed brand guidelines and approval tiers
- Hold a regular check-in, at least monthly, between communications, team leads, and leadership

Choosing the Right Platforms

The goal is strategic focus, not being everywhere. A smaller, well-run presence on the platforms where your actual audience spends time will always outperform a thin, inconsistent presence spread across every app that exists.

Where to focus

- **LinkedIn.** A primary hub for B2B relationships, recruiting, thought leadership, and executive visibility.
- **Facebook.** Still a strong hub for community, customer service, local reach, and event distribution.
- **Instagram.** A primary platform for visual brand storytelling, product content, and culture.
- **YouTube.** A durable home for tutorials, product demos, webinars, and long-form brand storytelling, and often a meaningful source of reach on its own.
- **TikTok or short-form video.** Increasingly relevant for reaching a younger or broader audience, worth a deliberate strategy rather than an afterthought.
- **Newsletter or podcast.** Often a core, owned part of the ecosystem, worth its own governance even though it isn't technically "social."
- **A social media management platform.** Tools like Sprout Social, Hootsuite, or Buffer, ideally with role-based access, are worth adopting so scheduling and approval can be centrally managed and audited.

A WORD OF CAUTION

New platforms, location accounts, or department-specific presences should go through the same review as any other organizational decision. An unmanaged account is a real security and reputational exposure, not just a minor inconsistency.

Multiple locations or departments, one governed standard

Every team, office, or franchise location should operate within one governed brand standard, set centrally, even if individual locations have some local flavor in their content. This should be a documented decision, with a clear path to follow if a team wants to deviate.

Account ownership

Every account, central, local, or leader-specific, should be owned under a company email address and managed through your scheduling tool wherever possible, with access governed by role, not by individual relationships.

Your Team & Account Inventory

An informal record of who has access to what is a real risk once more than one person touches your accounts. This page should be maintained as a living document, reviewed on a set schedule, and integrated into your broader IT and HR processes.

KEEP THIS PAGE SECURE

Because it will contain login information across your entire organization's social footprint, this page (or its digital equivalent) is the single most sensitive document in this guide. Store it in an access-controlled password manager, and treat every update to it as a required step in onboarding and offboarding.

Your social media team, in writing

DIRECTOR OF COMMUNICATIONS / MARKETING

PHONE

EMAIL

COMMUNITY / DIGITAL LEAD

PHONE

EMAIL

APPROVING LEADER (CEO / PRESIDENT)

PHONE

EMAIL

LEGAL / RISK MANAGEMENT CONTACT

PHONE

EMAIL

PASSWORD MANAGER / SYSTEM USED

DATE LAST REVIEWED

SECTION 04 CONTINUED

Your account inventory

List every account your organization operates, across every team, location, and platform, including your scheduling tool and any leader-specific accounts your team helps manage. An unmonitored account or lingering former-employee access is a real, avoidable exposure.

Platform / Team	Account Name	Linked Email	Username	Who Has Access
Company: LinkedIn				
Company: Facebook				
Company: Instagram				
Company: YouTube				
Company: TikTok				
Newsletter / Podcast				
Scheduling Tool				
Team / Location:				
Team / Location:				
Other:				

REDUNDANCY AND ACCOUNTABILITY

Every account should have at least two current employees with access, managed through role-based permissions rather than individually shared passwords wherever your tools allow it. Tie every update to this page directly to your HR and IT offboarding workflows.

Content Guidelines & Voice

The greatest risk to your content is not inconsistency of effort. It's the slow erosion of personality that happens as a content operation grows and becomes more polished. The organizations that stand out are the ones that still sound like real people, backed by real production value, rather than a stiff institutional account.

Govern your brand voice deliberately

Maintain a documented brand and style guide: tone, visual identity, example posts that represent you well, and examples that miss the mark. Every contributor should be trained on it, and it should be revisited at least annually as your organization evolves.

Balance your content categories

A healthy content mix draws from more than announcements and promotion. Rotate deliberately across these categories.

Category	Examples
Culture & people	Employee spotlights, behind-the-scenes moments, humor, what makes your organization distinct
Expertise & value	Industry insight, education, thought leadership, product or service value explained plainly
Community & stories	Customer stories, testimonials, case studies, real outcomes, always with consent
Promotion & logistics	Launches, offers, events, hours, links, announcements

A HELPFUL RATIO

If promotion and logistics make up more than a third of what your primary account posts in a given month, invest more in culture and expertise. Track this deliberately through your content calendar, not just anecdotally.

What to avoid

- Partisan political endorsements or commentary from any official company account
- Unvetted, hot-button debates in comment threads
- Specific nonpublic financial details, pricing negotiations, or a customer's or employee's personal hardship
- Details about someone's personal struggle, health, or family situation without their explicit permission

A simple pre-post gut check

Before hitting publish, on any account, the poster should be able to answer yes to each of these: Does this sound like us? Would leadership be comfortable seeing this go live? Have we gotten permission from anyone named or shown? Is this something we would still be glad we posted a year from now?

Approval & Posting Workflow

A clearly tiered, documented approval process keeps routine content moving quickly while giving sensitive or brand-defining content a fast, well-understood path to the right decision-maker.

Post it directly (production team)

- Routine announcements, event promotion, and calendar updates, on any account
- Photos and video from routine activities, once media permissions are confirmed (see Section 07)
- Content already approved as part of a running campaign or content calendar

Get Director of Communications sign-off

- Any content introducing a new campaign, product, or brand element
- Paid promotion, sales campaigns, or pricing-related messaging
- Any response to public criticism or a negative comment thread that has gained real traction

Get Executive and Legal sign-off

- Anything naming a specific person in connection with hardship, loss, or a sensitive situation
- Anything related to a staff transition, layoff, discipline matter, or leadership change
- Any statement responding to a crisis, controversy, or media inquiry, coordinated with legal and, where appropriate, the board

KEEP THE PATH FAST

Even with a formal tiered process, sensitive content should never wait on more than a small, defined group of decision-makers. Document who those people are and their backup contacts, so approval never stalls because one person is unreachable.

A real editorial rhythm

A regular content review, weekly at the team level and monthly at the leadership level, keeps your content aligned across every team and platform, and surfaces brand or tone drift before it becomes a pattern.

Protecting People: Employees, Customers & Minors

This is the single most important section of this guide, regardless of your industry or size. Getting this wrong doesn't just create a bad post. It can create real legal exposure and real, lasting harm to a real person.

The core rule

Never post a photo, video, testimonial, or story that identifies an employee, customer, or minor without documented consent. This applies to marketing content, case studies, employee spotlights, event coverage, and any content involving a recognizable person, on every account.

Getting permission the right way

A verbal understanding is never sufficient. Permission should be captured in writing, whether through a signed release form, a check-in system, a customer agreement, or an HR record, and refreshed periodically for anyone in an ongoing relationship with your brand.

- Use plain, unambiguous language a person can say yes or no to without feeling pressured, for example: "I give permission for my photo, video, or story to be used by [Company Name] in social media, website, and marketing materials."
- Ensure a real, honored opt-out is visible to every photographer, event staffer, and content producer, not just the central communications team
- Renew standing permissions on a set schedule, especially for employees, brand ambassadors, or repeat customers featured regularly

IF MINORS ARE EVER PART OF YOUR CONTENT

If your organization's events, products, or marketing ever involve minors, family programs, youth partnerships, camps, or school relationships, apply this standard with extra rigor. Never post a photo or video that clearly identifies a minor without written permission from a parent or legal guardian, even if the child only appears in the background of a group shot.

SECTION 07 CONTINUED

Review every photo before it posts, not just for permission

Getting permission is only half the job. Before any photo or video goes live, someone trained on this standard should look at it closely, with these questions in mind:

- Is everyone in the frame, including in the background, covered by permission? Group shots often catch people whose consent was never given.
- Is anyone doing something embarrassing, unsafe, or simply not how they would want to be remembered? A candid moment is charming. A moment someone would be humiliated by later is not.
- Is there anything in the background that should not be public? Screens showing customer data, whiteboards with sensitive information, ID badges, addresses, or an unlocked door are common, avoidable mistakes.
- Does the image show an injury, a medical situation, or a vulnerable moment? Those moments deserve privacy, not an audience, and definitely not a caption.

A SIMPLE STANDARD

Ask yourself: would I be comfortable if this exact photo were the first thing this person saw about themselves today? If there is any hesitation at all, do not post it.

Keep a centralized opt-out list

Maintain one centralized, auditable opt-out list, accessible to every team involved in content production, rather than separate lists that can fall out of sync.

Additional safeguards

- Never include a person's full name alongside their photo unless they have specifically approved it
- Avoid posting details that reveal someone's home address, school, or daily routine
- When in doubt, crop the photo, blur faces, or simply choose a different image
- Apply the same care to anyone in a sensitive personal, medical, or legal situation

Managing Comments & Public Interaction

Comment and message volume is often heavier than expected, and slow or inconsistent responses are far more visible than most organizations realize. This deserves a documented process with real ownership behind it.

Response expectations

Aim for same-day, if not same-hour, responses on primary accounts, and within 24 hours on secondary or local accounts. Use your social media management platform to assign clear ownership and track response times across every account and contributor.

Handling criticism

- Stay calm and professional, even when a comment feels unfair or pointed
- Never argue with someone publicly in the comments, on any account
- Move sensitive or heated conversations to a private message, phone call, or in-person meeting
- If a comment raises a legitimate concern, thank the person for raising it and follow up privately
- Escalate any comment thread gaining real traction, or drawing outside or media attention, directly to the Director of Communications

When to remove a comment

Leave it and respond	Remove or hide it
Honest disagreement or criticism, even if uncomfortable	Profanity, harassment, or personal attacks on staff or customers
Questions about your products, practices, or policies	Spam, scams, or promotional links
A complaint stated respectfully	Content that discloses someone's private information without consent

When Things Go Wrong: A Basic Crisis Protocol

A difficult moment can reach far beyond your usual audience fast: a safety incident, a product or service failure, a leadership controversy, a data issue, or a post that goes viral for the wrong reasons and draws sustained media attention.

Your basic first steps

1. **Pause scheduled content, everywhere.** Turn off any automated or pre-scheduled posts across every account and platform.
2. **Notify leadership and legal immediately.** Executive leadership, the Director of Communications, and your legal or risk management contact should know within minutes.
3. **Name one spokesperson.** Only one person should speak publicly on behalf of the organization, in comments, in messages, and to any media, and that person should be pre-identified, not chosen in the moment.
4. **Do not respond publicly until leadership, legal, and communications agree on a message.** A rushed, unapproved comment anywhere can materially worsen a serious situation.
5. **Keep any statement factual, brief, and measured.** Acknowledge what you know, avoid speculation, and share next steps if appropriate.
6. **Loop in your board or ownership and any external PR or crisis counsel per your existing governance process.** That conversation should happen early and in parallel with your public response, not after it.

THIS IS A STARTING POINT, NOT A FULL PLAN

A true crisis communication plan includes pre-approved statement templates, a documented notification chain, media response protocols, legal and PR coordination, spokesperson training, and regular practice drills. This guide gives you the basics. UNCOM Media specializes in building the complete plan alongside your leadership team, so you are never figuring this out for the first time in the middle of an actual crisis.

Account Security Basics

Organizations of every size are a real target for hacking, impersonation, and coordinated harassment, given their visibility. Security here should be treated as a real IT function, not an informal habit, built on the account inventory you completed in Section 04.

- **Use an access-controlled password manager.** With permission tiers so employees only access what their role requires.
- **Keep at least two admins on every account.** Managed through role-based access, not individually shared credentials, wherever your tools support it.
- **Turn on two-factor authentication with no exceptions.** Across every account and every platform.
- **Tie every account to a company email address and your IT identity system.** Never a personal one, with access removed automatically as part of offboarding wherever possible.
- **Integrate access changes into your formal HR and IT offboarding workflow.** This should be a required, tracked step, not a manual afterthought.
- **Conduct a documented quarterly access review.** Given the number of accounts and employees involved, this review should be a standing item for your communications and IT leadership.
- **Monitor for impersonation and coordinated harassment.** Fake accounts and organized negative campaigns are a real possibility worth having a documented response plan for.

Copyright & Legal Basics

Real legal review of your content practices is worth budgeting for as a standing relationship, not a one-time consultation.

- **License your music properly.** Use a licensed music library, such as Epidemic Sound, Artlist, or a comparable sync license, for anything used in commercial or promotional video.
- **Use licensed or free stock images and footage.** Do not pull images or video directly from a search engine. Use royalty-free sources or media your organization has purchased or been given rights to use.
- **Use model and media releases for larger events.** Especially anything professionally photographed, filmed with drones, livestreamed, or used in paid promotion.
- **Follow disclosure requirements for sponsored or paid content.** Any paid partnership, affiliate link, or influencer collaboration should follow applicable advertising disclosure rules in your market.
- **Protect your brand and trademarks.** Your organization's name, logo, and distinct branding are worth formally protecting, and your legal counsel should be aware of how they are used across teams and partners.
- **Give credit where it is due.** If you share someone else's content, tag or credit the original creator.
- **Do not screenshot and repost without permission.** Especially from other organizations, journalists, or creators.

NOTE

This section covers general best practices only, not legal advice. An ongoing relationship with an attorney familiar with your industry and media law is a reasonable investment, not a luxury.

Sample Policy Statement & Staff Agreement

Below is a short, adaptable statement your organization can copy, adjust to fit your context, and have every employee or contractor with social media access sign.

[Company Name] Social Media Policy & Agreement

_____ agrees to serve as _____ (role) for [Company Name], managing the _____ account(s), and in this role agrees to:

- Represent the organization's voice and personality with honesty and care in every post and interaction, in line with the documented brand guide
- Obtain written permission before posting any photo, video, or story that identifies an employee, customer, or minor, and review every photo for appropriateness before it goes live
- Route any content requiring sign-off, as outlined in Section 06, to the appropriate approving leader before posting
- Avoid posting partisan political content, unverified claims, or private information about any employee, customer, or company matter
- Coordinate personal social media use with the communications team when in a public-facing role, understanding it may be closely associated with the organization
- Respond to comments and messages with professionalism, and escalate any hostile, coordinated, or concerning interaction to the Director of Communications
- Follow the organization's crisis communication protocol and pause posting immediately if instructed by leadership
- Keep the Account Inventory (Section 04) accurate and secure, and report any suspected unauthorized access immediately

Signature

Date

Quick-Start Checklist

Use this checklist to put the basics of this guide into practice this quarter.

- ☐ Formalize the Director of Communications, production team, Community/Digital lead, Approving Leader, and legal contact in writing
- ☐ Complete the Team & Account Inventory in Section 04 across every platform and location, and store it in an access-controlled system
- ☐ Confirm every account is owned under a company email, with role-based access, at least two admins, and two-factor authentication turned on with no exceptions
- ☐ Adopt or fully utilize a social media scheduling and management platform
- ☐ Document a real brand and style guide, and train every contributor on it
- ☐ Build a documented content pipeline and shared content calendar with visibility across every team
- ☐ Move photo, video, and testimonial consent tracking into an audited system, with one centralized opt-out list
- ☐ Assign a specific role responsible for auditing media consent compliance across every team
- ☐ Define your tiered approval process, including legal and leadership escalation for crisis-level content
- ☐ Integrate account access changes directly into your formal HR and IT offboarding workflows
- ☐ Schedule a quarterly access review, a monthly leadership content review, and a weekly team-level check-in
- ☐ Review the basic crisis protocol in Section 09 with leadership and legal counsel, and identify your PR or crisis communications partner in advance
- ☐ Have every employee or contractor with social media access sign the policy agreement in Section 12



You've Got the Basics. Let's Build the Rest.

This guide covers the fundamentals every organization needs. But every team, no matter how well-run, eventually faces a moment it did not fully plan for: a crisis, a controversy, a hard conversation that plays out across platforms and potentially national media at once. That is exactly what we help organizations prepare for.

UNCOM Media builds custom social media policies, crisis communication plans, and leadership training for organizations of every size and industry. If you would like help turning this guide into a complete, board-ready plan built specifically for your team, we would love to talk.

WWW.UNCOM.MEDIA

rich@uncom.media

(469) 513-1040

CLARITY • CONSISTENCY • TRUST