Retail Employee Social Media Policy Template

A practical, editable policy framework for retailers, store teams, ecommerce teams, and public-facing employees

Use this template as a starting point, then edit the placeholders, reporting contacts, approval workflows, and legal language for your company.

Prepared for: [Company Name]

Version: [Version Number] | Effective Date: [Date] | Owner: [Department or Role]

Template note: This document is not legal advice. Retailers should review this policy with counsel and adapt it to local, state, federal, and country-specific employment laws.

Table of Contents

Tip: Replace every bracketed field, including [Company Name], [Department or Role], [Contact Email or Channel], [HR Contact], [Legal Contact], and [Security Contact].

How to use this template

This policy is written for retailers and can be edited for store teams, ecommerce teams, distribution centers, corporate employees, managers, contractors, and public-facing roles. Replace bracketed placeholders and remove any section that does not fit your business.

1. Purpose

[Company Name] understands that employees use social media every day to connect with others, share opinions, follow brands, discuss products, and participate in online communities.

This policy explains how employees should use social media when their activity may relate to [Company Name], our stores, customers, coworkers, products, vendors, business partners, or reputation.

The goal is not to control every personal post. The goal is to help employees use social media responsibly, protect customer and company information, avoid confusion about who speaks for [Company Name], and reduce legal, security, HR, and brand risk.

2. Who this policy applies to

This policy applies to all [Company Name] employees, including:

- Full-time employees
- Part-time employees
- Seasonal employees
- Temporary employees
- Store employees
- Corporate employees
- Warehouse and distribution employees
- Managers and supervisors
- Remote employees
- Interns
- Contractors and agency workers acting on behalf of [Company Name]

This policy applies to personal social media use when posts relate to [Company Name], work, customers, coworkers, products, stores, promotions, vendors, or company information. It also applies to official [Company Name] social media accounts and any social media use involving company devices, systems, networks, photos, logos, or materials.

3. Platforms covered by this policy

This policy applies to social media platforms, messaging apps, online communities, forums, review sites, video platforms, comment sections, and other digital spaces.

- Facebook
- Instagram

- TikTok
- X
- LinkedIn
- Reddit
- Discord
- YouTube
- Snapchat
- Threads
- Pinterest
- WhatsApp
- Slack
- Microsoft Teams
- Blogs
- Review sites
- Forums
- Private groups
- Online marketplaces
- Any future platform where employees post, comment, share, message, stream, or upload content

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

4. Personal accounts vs. official company accounts

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

Only authorized employees may post from official [Company Name] social media accounts or speak publicly on behalf of [Company Name].

Employees may not create accounts, pages, groups, usernames, or profiles that appear to represent [Company Name], a [Company Name] store, a company department, or a company brand unless approved by [Department or Role].

Employees may not use [Company Name] logos, trademarks, store images, product photos, uniforms, internal documents, or brand assets in a way that suggests official approval unless authorized.

5. Disclose your connection to [Company Name]

Employees should be honest about their connection to [Company Name] when posting about company-related matters.

If an employee discusses [Company Name], our products, our services, our competitors, our promotions, our customers, or industry topics connected to their role, they should disclose that they work for [Company Name].

Example wording:

- I work for [Company Name], but these are my own views.
- I'm a [Company Name] employee, and this is my personal opinion.
- I work at [Company Name], but I'm not speaking on behalf of the company.

Employees may not review, recommend, defend, or promote [Company Name] products or services in a way that hides their employment relationship.

6. Do not speak for [Company Name] unless authorized

Unless specifically approved, employees may not speak on behalf of [Company Name].

Employees should avoid phrases such as:

- [Company Name] wants everyone to know...
- Our official position is...
- We are announcing...
- On behalf of [Company Name]...
- The company will...

Employees should refer media requests, legal questions, investor questions, customer escalations, public complaints, or crisis-related issues to [Department or Role].

7. Protect confidential company information

Employees may not post, upload, livestream, screenshot, forward, or share confidential or non-public company information.

Confidential information may include:

- Sales numbers
- Store performance data
- Revenue or financial information
- Inventory information
- Pricing strategy
- Vendor terms
- Product launch plans
- Promotion calendars
- Future ads or campaigns
- Internal emails or messages
- Store operations documents
- Security procedures
- Loss prevention information
- Internal investigations

- Legal matters
- Employee records
- Customer information
- Non-public company announcements
- Business plans or strategy

If information is not already public, employees should not be the ones to make it public. When in doubt, do not post it. Ask [Department or Role] first.

8. Protect customer privacy

Employees must never share customer personal information online.

- Customer names
- Phone numbers
- Email addresses
- Home addresses
- Payment information
- Order details
- Receipts
- Account information
- Loyalty program information
- Delivery details
- Return details
- Customer service conversations
- Photos or videos of customers without approval
- Private complaints or disputes

Employees should not post about specific customer situations, even if the customer's name is not included, if the customer could reasonably be identified.

Employees may not shame, mock, insult, expose, record, or photograph customers for social media content.

9. Respect coworkers, customers, vendors, and competitors

Employees are expected to follow [Company Name] conduct standards online just as they would at work.

Employees may not use social media to harass, threaten, bully, intimidate, discriminate against, dox, or target coworkers, customers, vendors, competitors, job applicants, or members of the public.

Prohibited conduct may include:

- Racist comments
- Sexist comments
- Religious harassment
- Disability-related harassment

- Age-related harassment
- Sexual harassment
- Threats of violence
- Bullying
- Posting private information about others
- Mocking customers or coworkers
- Encouraging harassment by others
- Sharing offensive images, memes, or videos tied to protected characteristics
- Retaliating against someone for reporting a workplace concern

This policy applies even when the post is made from a personal account or outside work hours if the conduct affects the workplace, customers, employees, or [Company Name].

10. Employee rights are respected

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

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

Employees should still avoid sharing customer information, trade secrets, private employee records, confidential business information, or security-sensitive information when discussing workplace concerns.

11. Social media use during work

Employees should not use personal social media during work time unless permitted by their manager or required for their job.

Social media use must not interfere with:

- Customer service
- Safety
- Productivity
- Job duties
- Store operations
- Warehouse or distribution work
- Driving or equipment use
- Meetings
- Training
- Supervision

Company devices, networks, and systems should be used according to [Company Name] technology and acceptable use policies.

12. Photos, videos, and recordings at work

Employees may not take or post photos, videos, livestreams, or recordings in restricted or private areas unless authorized.

Restricted areas may include:

- Stockrooms
- Offices
- Break rooms
- Security areas
- Warehouses
- Distribution centers
- Registers
- Customer service desks
- Inventory areas
- Loading docks
- Employee-only areas
- Areas showing customer information
- Areas showing security equipment or internal operations

Employees should not record coworkers, customers, vendors, or visitors without permission where required by law or company policy.

Employees should not create social media content that interferes with work, customer privacy, safety, or operations.

13. Promotions, contests, discounts, and product claims

Employees may not create or advertise promotions, contests, giveaways, coupons, discounts, sweepstakes, or special offers on behalf of [Company Name] unless authorized.

Employees may not make false, misleading, exaggerated, or unapproved claims about:

- Products
- Services
- Pricing
- Warranties
- Product availability
- Delivery timelines
- Competitors
- Promotions
- Return policies
- Discounts
- Loyalty programs

Employees should not promise special treatment, unauthorized discounts, refunds, or product availability outside company rules.

All promotions, contests, giveaways, and marketing claims must be approved by [Department or Role].

14. Reviews, ratings, and endorsements

Employees may not post fake reviews, misleading reviews, or anonymous endorsements of [Company Name], competitors, vendors, or products.

If employees review, recommend, defend, or promote [Company Name] products or services online, they must disclose that they work for [Company Name].

Employees may not pressure coworkers, family members, friends, vendors, or customers to post positive reviews.

Employees may not offer unauthorized rewards, discounts, gifts, or benefits in exchange for reviews.

15. Legal, financial, and crisis-related matters

Employees may not post about legal matters, lawsuits, investigations, accidents, security incidents, data incidents, executive decisions, financial results, public controversies, or crisis situations involving [Company Name] unless authorized.

Employees should not respond publicly to reporters, influencers, activists, attorneys, regulators, competitors, or public complaints on behalf of [Company Name] unless it is part of their approved role.

If contacted by the media or asked to comment publicly on company matters, employees should refer the request to [Department or Role].

16. Competitors, vendors, and business partners

Employees should be respectful when discussing competitors, vendors, suppliers, manufacturers, delivery partners, marketplace sellers, or other business partners.

Employees may not share confidential information about competitors, vendors, suppliers, or partners learned through their work.

Employees should not make false, misleading, insulting, or unverified claims about competitors or their products.

Employees should not disclose vendor pricing, contract terms, negotiations, supply issues, private meetings, or confidential business terms.

17. Managers and supervisors

Managers and supervisors have additional responsibilities.

Managers should not:

- Pressure employees to connect on personal social media accounts
- Ask employees or applicants for social media passwords
- Use personal social media to harass, monitor, intimidate, or retaliate against employees
- Discuss private employee matters online
- Post about employee discipline, performance, attendance, accommodations, complaints, investigations, or terminations
- Encourage employees to post company content without proper disclosure
- Retaliate against employees for protected workplace discussions

Managers should model good judgment and contact [Department or Role] when unsure how to handle a social media issue.

18. Official company accounts

Only authorized employees may manage or post from official [Company Name] social media accounts.

Employees with official account access must:

- Use approved login and security procedures
- Use multi-factor authentication where required
- Follow brand guidelines
- Use approved images, videos, music, and copy
- Respect copyright and trademark rules
- Protect customer information
- Follow approval workflows
- Avoid personal opinions from official accounts
- Escalate sensitive issues quickly
- Report account access problems immediately
- Never share passwords outside approved systems

When an employee leaves [Company Name] or changes roles, access to official accounts must be removed promptly.

19. Security, scams, and impersonation

Employees should be alert for scams, phishing attempts, impersonation, fake accounts, suspicious links, and social engineering.

Employees should report:

- Fake [Company Name] accounts
- Impersonation of employees, executives, stores, or customer support accounts
- Suspicious messages asking for company information
- Requests for passwords or login codes
- Fraudulent promotions or coupons

- Fake customer service accounts
- Account takeovers
- Security incidents involving social media

Report concerns to [Department or Role].

20. Copyright, trademarks, and content ownership

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

- Music
- Videos
- Photos
- Memes
- Logos
- Artwork
- Product images
- Customer content
- Vendor content
- Internal company materials
- Training materials
- Screenshots from company systems

Employees may not misuse [Company Name] trademarks, logos, slogans, product names, store images, or brand assets.

21. When to ask for help

Employees should ask for guidance before posting if the content involves:

- Confidential information
- Customer information
- Internal company matters
- Legal issues
- Financial information
- Promotions or discounts
- Media requests
- Complaints about customers or coworkers
- Company logos or trademarks
- Product claims
- Security issues
- Sensitive workplace topics
- Anything that could be mistaken for an official company statement

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

22. Reporting concerns

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

- Disclosure of customer information
- Disclosure of confidential company information
- Harassment or threats involving coworkers or customers
- Fake company accounts
- Scams or impersonation
- Unauthorized use of company logos
- Posts that appear to speak for the company without approval
- Security risks
- Legal or media issues
- Unauthorized promotions or product claims

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

[Company Name] prohibits retaliation against employees who report concerns in good faith.

23. Policy violations

Violations of this policy may result in corrective action, up to and including termination of employment, depending on the circumstances and applicable law.

Examples of violations may include:

- Sharing confidential company information
- Sharing customer personal information
- Harassing coworkers or customers online
- Speaking for [Company Name] without authorization
- Posting false or misleading product claims
- Posting unauthorized promotions or contests
- Misusing company logos or trademarks
- Using official accounts without approval
- Sharing account passwords
- Posting content that violates company conduct policies
- Retaliating against employees for protected activity or good-faith reporting

[Company Name] will review each situation based on the facts, applicable law, company policy, and business impact.

24. Related policies

Employees should also review and follow related [Company Name] policies, including:

- Code of Conduct

- Employee Handbook
- Confidentiality Policy
- Information Security Policy
- Customer Privacy Policy
- Anti-Harassment and Anti-Discrimination Policy
- Workplace Violence Policy
- Media Relations Policy
- Marketing and Promotions Policy
- Acceptable Use of Technology Policy
- Copyright and Trademark Policy
- Data Privacy Policy
- Records Retention Policy
- Disciplinary Action Policy

25. Employee acknowledgment

I acknowledge that I have received and reviewed the [Company Name] Employee Social Media Policy. I understand that I am responsible for following this policy when using social media in ways that relate to [Company Name], its customers, employees, business partners, products, services, stores, or reputation.

I understand that this policy does not prevent me from exercising rights protected by applicable law, including rights related to wages, hours, working conditions, protected concerted activity, reporting legal concerns, or participating in investigations.

Employee Name	
Employee Signature	
Date	
Manager or HR Representative	