EMPLOYEE SOCIAL MEDIA POLICY TEMPLATE

For Financial Services Companies

A practical policy template for employee social media use, official company accounts, customer privacy, confidentiality, compliance, financial communications, and online conduct.

Company: [Company 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, compliance, HR, privacy, security, and communications teams before use. It is not legal advice.

Table of Contents

Policy Summary for Employees

- Be clear when you are speaking for yourself and not for [Company Name].
- Disclose your connection to [Company Name] when discussing company-related products, services, or industry topics.
- Never share customer, client, investor, account, transaction, confidential, non-public, or market-sensitive information.
- Do not provide unauthorized financial advice, product recommendations, investment commentary, or performance promises.
- Use official accounts only if authorized, and follow approval, security, archiving, and recordkeeping procedures.
- Ask [Department or Role] before posting about legal, regulatory, financial, security, crisis, media, or customer matters.

Important

This policy should be adapted for the specific rules that apply to your business, including banking, broker-dealer, investment advisory, insurance, lending, privacy, advertising, supervision, recordkeeping, and employment law requirements.

1. Purpose

[Company Name] recognizes that employees use social media to communicate, build professional networks, share opinions, follow financial news, and participate in online communities.

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

The goal is not to control personal expression. The goal is to protect confidential information, customer privacy, market integrity, regulatory compliance, and public trust.

2. Who this policy applies to

This policy applies to all [Company Name] workforce members, including full-time, part-time, temporary, remote, hybrid, intern, contractor, consultant, agency, advisor, and representative personnel when acting on behalf of [Company Name].

It applies to personal social media use when posts relate to [Company Name], our business, financial products, clients, coworkers, competitors, markets, investments, or work-related matters. It also applies to official [Company Name] social media accounts and any social media use involving company devices, systems, networks, logos, or materials.

3. Personal accounts vs. official company accounts

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

Only authorized employees may post from official [Company Name] 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 business unit, branch, product, service, or advisory team unless approved by [Department or Role].

Employees may not use [Company Name] logos, trademarks, product names, client-facing materials, internal screenshots, or brand assets in a way that suggests official approval unless authorized.

4. Disclose your connection to [Company Name]

Employees should be transparent about their relationship with [Company Name] when posting about company-related matters, financial products, services, industry topics, partners, or competitors connected to their role.

Examples of simple disclosures include: "I work for [Company Name], but these views are my own," "I am a [Company Name] employee, and this is my personal opinion," or "I am not speaking on behalf of [Company Name]."

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

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

Employees may not present personal opinions as official company statements. Unless specifically authorized, employees should not use language such as "[Company Name] believes," "our official position is," "we are announcing," or "on behalf of [Company Name]."

Media inquiries, investor questions, analyst requests, regulator inquiries, legal questions, public complaints, and crisis-related issues should be referred to [Department or Role].

6. Protect confidential and non-public information

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

Confidential information may include financial results, earnings information, forecasts, business strategy, acquisition or partnership discussions, product plans, pricing strategy, client lists, customer data, account information, internal reports, risk models, legal matters, investigations, compliance reviews, security procedures, and non-public announcements.

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

7. Protect customer, client, and investor privacy

Employees must never share private customer, client, investor, account, transaction, or financial information online.

This includes names tied to account details, account numbers, balances, transactions, holdings, loan details, insurance details, payment information, contact information, credit information, tax information, support tickets, private messages, screenshots from internal systems, or details that could identify a customer or client.

Employees should not describe a customer situation online, even without a name, if the person or organization could reasonably be identified.

8. Financial advice, recommendations, and product claims

Employees may not provide financial, investment, tax, insurance, lending, banking, or legal advice on social media unless it is part of an approved job responsibility and follows [Company Name] procedures.

Employees may not make false, misleading, exaggerated, or unapproved claims about returns, performance, rates, fees, risk, guarantees, investment outcomes, insurance coverage, lending approvals, credit decisions, or product availability.

Employees should direct individuals seeking advice or service support to approved [Company Name] channels.

9. Market, trading, and securities information

Employees may not post non-public information that could affect markets, investors, securities, trading, customers, or business partners.

Employees may not discuss restricted information, trading activity, research, investment banking matters, client transactions, pending deals, internal views, or market-sensitive information unless authorized and compliant with company policy.

Employees must follow all applicable insider trading, market conduct, research, communications, and information barrier policies.

10. Advertising, endorsements, reviews, and testimonials

Employees may not post fake reviews, misleading reviews, anonymous endorsements, undisclosed promotions, or testimonials that violate company policy or applicable law.

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

Employees may not offer unauthorized rewards, discounts, gifts, special terms, referral bonuses, product claims, or promotional promises through social media. Marketing, influencer, affiliate, and paid endorsement activity must be approved by [Department or Role].

11. Professional conduct online

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 customers, clients, coworkers, applicants, regulators, competitors, vendors, or members of the public.

This policy applies even when posts are made from personal accounts or outside work hours if the conduct affects customers, coworkers, the workplace, or [Company Name].

12. Employee rights are respected

Nothing in this policy is intended to prevent employees from discussing wages, hours, schedules, workplace safety, working conditions, benefits, union activity, 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 customer information, trade secrets, private employee records, confidential business information, security-sensitive information, or legally protected client information when discussing workplace concerns.

13. 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 procedures, multi-factor authentication, approved content, brand guidelines, disclosure language, supervision workflows, and recordkeeping procedures where required.

Employees must protect credentials, avoid personal opinions from official accounts, escalate sensitive issues quickly, and never share passwords outside approved systems. Account access must be removed promptly when an employee changes roles or leaves [Company Name].

14. Records, archiving, and compliance review

Financial services communications may be subject to recordkeeping, supervision, approval, or archiving requirements. Employees must follow [Company Name] procedures for business-related social media communications.

Employees may not use unapproved channels to conduct company business, discuss customer accounts, provide advice, negotiate terms, or make product recommendations.

Business communications that must be retained should occur only through approved systems and approved accounts.

15. Security, fraud, and impersonation

Employees should be alert for phishing, scams, fake accounts, impersonation, suspicious links, social engineering, account takeovers, and fraudulent financial promotions.

Employees should report fake [Company Name] accounts, impersonation of employees or executives, suspicious messages asking for company or customer information, requests for passwords or login codes, fraudulent offers, fake

customer support accounts, and social media account compromises to [Security Contact or Department].

16. 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 offices, trading floors, customer meeting rooms, call centers, branches, data centers, records areas, screens showing customer data, security areas, and employee-only areas.

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

17. Managers, leaders, and public-facing employees

Managers, executives, advisors, recruiters, sales employees, relationship managers, and public-facing employees may create greater risk because their posts are more likely to be associated with [Company Name].

Managers should not pressure employees to connect on personal accounts, ask for passwords, discuss private employee matters online, retaliate for protected workplace discussions, or make public statements that appear to represent [Company Name] unless authorized.

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

18. Competitors, partners, and vendors

Employees should be respectful when discussing competitors, partners, vendors, affiliates, issuers, counterparties, or industry peers.

Employees may not share confidential information learned through work, including private business terms, pricing, negotiations, contracts, client relationships, partner roadmaps, or integration details.

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

19. Use of AI-generated content

Employees should be careful when using AI tools to create social media content related to [Company Name], financial services, customers, markets, or regulated products.

Employees may not enter confidential company information, customer information, account data, financial records, private documents, security details, or non-public business information into unapproved AI tools.

AI-generated content for official accounts must follow review and approval processes. Employees are responsible for checking AI-generated content for accuracy, confidentiality issues, bias, copyright concerns, and misleading claims before posting.

20. Reporting concerns

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

Examples include disclosure of customer information, confidential information, harassment, fake company accounts, impersonation, scams, security risks, unauthorized product claims, unauthorized media comments, or use of official accounts without approval.

Reports can be made to [Department or Role], [Security Contact], [Compliance Contact], [HR Contact], [Legal Contact], or [Anonymous Reporting Channel]. [Company Name] prohibits retaliation against employees who report

concerns in good faith.

21. When to ask for help

Employees should ask [Department or Role] before posting if content involves customer information, financial advice, investment commentary, market-sensitive information, legal matters, regulatory issues, product claims, official statements, promotions, media requests, customer complaints, confidential information, company logos, or anything that could be mistaken for an official company statement.

Questions can be sent to [Contact Email or Channel].

22. Policy violations

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

Examples include sharing customer information, disclosing confidential company information, providing unauthorized financial advice, speaking for [Company Name] without authorization, posting misleading claims, harassing others online, misusing company logos, using official accounts without approval, sharing passwords, and retaliating against protected activity or good-faith reporting.

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

23. 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, Communications and Marketing Policy, Anti-Harassment and Anti-Discrimination Policy, Records Retention Policy, Acceptable Use of Technology Policy, Insider Trading Policy, Media Relations Policy, AI Use Policy, Incident Reporting Policy, and Disciplinary Action Policy.

24. 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, clients, employees, products, services, business partners, 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: _____