EMPLOYEE SOCIAL MEDIA POLICY TEMPLATE

For Technology Companies

A practical policy template for employee social media use, official company accounts, confidentiality, privacy, security, product communication, 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, HR, privacy, security, and communications teams before use. It is not legal advice.

Table of Contents

1. Purpose
2. Who this policy applies to
3. Personal accounts vs. company accounts
4. Disclose your connection to [Company Name]
5. Do not speak for [Company Name] unless authorized
6. Protect confidential information
7. Respect customer, user, and employee privacy
8. Be accurate and honest
9. Follow workplace conduct rules online
10. Respect employee rights
11. Security, vulnerabilities, and incidents
12. Product, engineering, and developer community participation
13. Official company accounts
14. Public complaints, media, and crisis situations
15. Competitors, partners, and vendors
16. Reviews, endorsements, and promotions
17. Use of AI-generated content
18. Managers and leaders
19. Copyright, trademarks, and third-party content
20. Reporting concerns
21. When to ask for help
22. Policy violations
23. Related policies
24. Employee acknowledgment

1. Purpose

[Company Name] recognizes that employees use social media to communicate, learn, share ideas, build professional networks, and participate in online communities.

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

The goal of this policy is not to control personal expression. The goal is to help employees communicate responsibly, protect confidential information, avoid confusion about who speaks for [Company Name], and reduce legal, security, privacy, and brand risk.

2. Who this policy applies to

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

This policy applies to social media use that may relate to [Company Name], official company accounts, online forums, developer communities, messaging platforms, review sites, blogs, video platforms, public comment sections, company devices or networks, and any online activity that may affect [Company Name] or its business interests.

3. Personal accounts vs. 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 speak on behalf of [Company Name] or post from official company accounts.

Employees may not create accounts, pages, groups, channels, usernames, or profiles that appear to represent [Company Name], a [Company Name] product, or a [Company Name] team unless they have written approval from [Department or Role].

Employees may not use [Company Name] logos, trademarks, product names, screenshots, code names, internal images, interface designs, 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.

If an employee discusses [Company Name], its products, services, technology, competitors, customers, partners, industry topics related to their role, or company-sponsored initiatives, they should disclose their connection to [Company Name].

- Example: "I work for [Company Name], but these views are my own."
- Example: "I am a [Company Name] employee, and this is my personal opinion."

- Example: "I work on [general team or product area], but I am not speaking for [Company Name]."

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

Employees involved in marketing, developer relations, sales, recruiting, product, partnerships, or customer success should be especially careful to disclose their affiliation when posting about [Company Name] or related industry topics.

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

Employees may not present personal opinions as official company statements. Unless approved to speak on behalf of [Company Name], employees should not use language such as:

- [Company Name] believes...
- Our official position is...
- We are announcing...
- The company will...
- On behalf of [Company Name]...

Employees should refer media inquiries, investor questions, legal questions, analyst requests, government inquiries, and crisis-related questions to [Department or Role].

6. Protect confidential information

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

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

- Source code, product roadmaps, unreleased features, internal tools, security procedures, vulnerability details, and incident response information
- Customer data, user data, partner data, vendor terms, financial information, sales numbers, pricing strategy, and business strategy
- Acquisition or partnership discussions, internal emails or messages, design files, prototype screenshots, internal dashboards, private meeting notes, legal matters, personnel information, and non-public announcements

7. Respect customer, user, and employee privacy

Employees must not share private information about customers, users, coworkers, job candidates, vendors, partners, or community members.

Employees should not describe a customer, user, candidate, or employee situation in a way that allows the person or organization to be identified.

- Do not post customer or user names tied to private issues, account information, email addresses, phone numbers, payment information, support tickets, private messages, or internal system screenshots.

- Do not post customer usage data, bug reports that identify customers, security incidents involving customers or users, employee records, candidate information, or internal HR matters.
- Do not post photos or videos from private workspaces without approval.

8. Be accurate and honest

Employees should not post false, misleading, exaggerated, or unverified statements about [Company Name], its products, competitors, partners, customers, or industry matters.

Employees should not make promises about product features, launch dates, pricing, availability, performance, security, privacy, compliance, roadmap decisions, customer outcomes, service guarantees, or support commitments unless authorized.

If an employee is unsure whether a claim is accurate or approved, they should not post it.

9. Follow workplace conduct rules online

[Company Name] expects employees to follow company conduct standards online just as they would at work.

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

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

- Do not post content that targets a protected status or violates anti-harassment and anti-discrimination policies.
- Do not use personal accounts to intimidate, retaliate against, or shame coworkers, applicants, customers, users, or partners.
- Do not encourage harassment or abuse by others.

10. Respect employee rights

Nothing in this policy is intended to prevent employees from discussing wages, hours, working conditions, workplace safety, benefits, management practices, 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 disclosing trade secrets, customer data, user data, private employee records, confidential business information, or security-sensitive 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.

11. Security, vulnerabilities, and incidents

Employees may not post about security incidents, vulnerabilities, data incidents, exploits, internal investigations, or incident response activity unless authorized.

Employees should not share vulnerability details, exploit steps, internal security tools, security architecture, incident timelines, customer impact details, internal investigation updates, access controls, passwords, keys, tokens, or credentials.

Phishing attempts or suspicious social media activity should be reported to [Security Contact or Channel]. If an employee discovers a security concern, they should follow [Company Name] security reporting process.

12. Product, engineering, and developer community participation

Employees may participate in developer communities, technical forums, open-source discussions, and professional networks when appropriate.

- Be respectful and accurate.
- Avoid sharing confidential information.
- Avoid implying official company approval unless authorized.
- Follow open-source, copyright, and licensing rules.
- Avoid discussing unreleased products or internal roadmaps.
- Make clear when views are personal.
- Escalate sensitive technical issues through approved channels.

Employees may not publish code, documentation, screenshots, product details, or internal technical information unless it is approved for public release.

13. Official company accounts

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

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

- Use approved login methods and multi-factor authentication.
- Protect credentials and never share passwords outside approved systems.
- Follow brand guidelines, approval workflows, and copyright and trademark rules.
- Avoid personal opinions from official accounts.
- Escalate sensitive comments or crises and report account access issues immediately.

14. Public complaints, media, and crisis situations

Employees should not respond on behalf of [Company Name] to public complaints, media inquiries, legal questions, regulatory issues, activist campaigns, customer disputes, or crisis events unless authorized.

Employees should escalate media requests, legal threats, regulatory questions, customer data concerns, security incidents, viral posts involving [Company Name], executive or employee controversies, product safety issues, public accusations, and coordinated harassment or abuse to [Department or Role].

15. Competitors, partners, and vendors

Employees should be respectful when discussing competitors, partners, vendors, suppliers, or industry peers.

Employees may not share confidential information about partners or vendors learned through work.

Employees should not make false, misleading, insulting, or unverified claims about competitors or their products. Employees should not disclose private business terms, negotiations, contracts, partner roadmaps, vendor pricing, or confidential integration details.

16. Reviews, endorsements, and promotions

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

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 discounts, incentives, giveaways, contests, referral rewards, product claims, or promotional promises. All campaigns, influencer work, affiliate relationships, contests, giveaways, and paid endorsements must be approved by [Department or Role].

17. Use of AI-generated content

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

Employees may not enter confidential company information, customer data, user data, source code, private documents, unreleased product information, or internal strategy into unapproved AI tools.

AI-generated content posted from official company accounts must follow [Company Name] approval processes. Employees are responsible for checking AI-generated content for accuracy, bias, copyright concerns, confidentiality issues, and misleading claims before posting.

18. Managers and leaders

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

- Do not pressure employees to connect on personal social media.
- Do not ask employees or applicants for passwords or private account access.
- Do not discuss private employee matters online.
- Do not post about employee discipline, performance, complaints, accommodations, investigations, or terminations.
- Do not retaliate against employees for protected workplace discussions.
- Do not 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.

19. Copyright, trademarks, and third-party content

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

This includes images, videos, music, memes, screenshots, logos, designs, product images, customer content, partner content, internal company materials, training materials, code, and documentation.

Employees may not misuse [Company Name] trademarks, product names, logos, interface designs, or brand assets.

20. Reporting concerns

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

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

- Disclosure of confidential information or customer or user data exposure
- Unauthorized company accounts, fake accounts, impersonation, account takeovers, or misuse of logos or trademarks
- Harassment, threats, security risks, unauthorized media statements, false product claims, or public posts involving legal, regulatory, or crisis matters

21. When to ask for help

Employees should ask [Department or Role] before posting if the content involves confidential information, customer or user information, legal matters, financial information, security issues, product roadmaps, unreleased features, company announcements, media requests, competitors, partners, promotions, AI-generated content, public complaints, workplace disputes, 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.

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

- Sharing confidential company information, customer or user data, or security-sensitive information
- Speaking for [Company Name] without authorization or using official accounts without approval
- Harassing coworkers, customers, users, or others online
- Posting false or misleading claims, unauthorized promotions, or endorsements
- Misusing company logos or trademarks, sharing account passwords, or retaliating against protected activity or good-faith reporting

23. Related policies

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

- Code of Conduct and Employee Handbook
- Confidentiality Policy and Information Security Policy
- Data Privacy Policy and Acceptable Use of Technology Policy
- Anti-Harassment and Anti-Discrimination Policy
- Media Relations Policy and AI Use Policy
- Security Incident Reporting Policy and Open Source Policy
- Copyright and Trademark Policy, Records Retention 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 employees, customers, users, partners, products, services, intellectual property, 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:	_____