**Social Media Policy Template**

# Guidance on the Appropriate Use of Social Media in the Workplace

## About This Social Media Policy

This social media policy provides guidance to employees regarding the recommended acceptable use of social media as it relates to their employment with **<<COMPANY>>.**

**<<COMPANY>> supports the rights of its employees to express themselves freely through social media.** These guidelines are not intended to infringe upon protected concerted activities that you as an employee and citizen have a right to engage in.

The guidelines provided in this document do not apply to an employee’s right to exercise their collective bargaining rights or any other freedoms or rights they have with respect to **<<LEGISLATION>>.**

Rather, this policy serves to establish expectations for professional conduct and provide employees with the best practices for representing **<<COMPANY>>** on social media in both official and unofficial capacities.

For example, employees retain their right to freely discuss their wages or working conditions. While grievances are best settled with direct communication between the employee and relevant parties, employees are free to express their grievances so long as their expression is truthful, lawful, and devoid of discrimination against protected classes.

Any concerns with this policy should be directed to **<<CONTACT>>** for further discussion.

### Scope

These guidelines apply to social media use from two key perspectives:

1. Employees, contractors, and consultants that use official **<<COMPANY>>** social media accounts to represent the company, and;
2. The professional conduct expectations of any associate that formally or informally represents **<<COMPANY>>** on their personal social media accounts.

For the purposes of this policy, **social media** is defined as sites and services that permit users to share information with other users. This includes, but is not limited to, blogs, online forums, wikis, chat rooms, newsletters, social networking sites, and other forms of electronic communication.

Examples of such sites and services include, but are not limited to, Facebook, LinkedIn, Twitter, Wikipedia, TikTok, and Reddit.

Throughout this policy **employees** will be used to collectively refer to employees, contractors, consultants, and other representatives of **<<COMPANY>>.**

## Social Media Use During Work Hours

While a reasonable amount of personal social media use is permitted during work hours, employees must ultimately act in the best interests of **<<COMPANY>>**. Personal use of social media must not interfere with your responsibilities as an employee. As such, disregarding job responsibilities and deadlines to use social media at work will not be tolerated.

**<<COMPANY>>** reserves the right to limit and monitor social media use during work hours through managerial and/or technical means.

All use of social media must abide by **<<COMPANY>>**’s existing policies, including but not limited to our Acceptable Use Policy, Discrimination & Harassment Prevention Policy, and **<<MENTION ANY RELEVANT COMPLEMENTARY SECURITY/CODES OF CONDUCT POLICIES HERE>>.**

## Guidelines on the Acceptable Use of Social Media

This section provides guidelines that employees should consider when using social media during their employment with **<<COMPANY>>**.

**<<COMPANY>>** supports the rights of its employees to express themselves freely through social media. This policy does not seek to unduly restrict the use of personal social media channels. However, employees must be cognizant of the fact that their online conduct may be seen as a representation of **<<COMPANY>>.**

Whether they are using social media in an official or unofficial manner, employees should use their best judgment in ensuring that they avoid posting material or engaging in conduct that is inappropriate or harmful to **<<COMPANY>>**, its employees, customers, and other stakeholders.

Such prohibited material or conduct includes commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can otherwise create a hostile work environment.

### Tone, Messaging, and Attitude

* All employees are expected to conduct themselves professionally in their online activities. All policies and expectations which apply to an employee’s offline conduct also apply to their online communications when representing **<<COMPANY>>**.
* Discriminatory remarks, harassment, and threats of violence will not be tolerated and may subject you to disciplinary action up to and including termination.
* When speaking with or about your colleagues any defamatory, offensive or derogatory content or statements may be subject to **<<COMPANY>>’s** Discrimination & Harassment Prevention Policy, even when made on your personal accounts.

### Company Representation & Conflicts of Interest

* Employees must be cognizant of the fact that anything shared on the internet can be readily duplicated and spread beyond their intended audience. Therefore, their local posts can have an unintentional global significance.
* When using social media for personal use you must not represent yourself as a spokesperson for **<<COMPANY>>** without prior approval.
* When referencing **<<COMPANY>>** in your online communications, be transparent about your association with **<<COMPANY>>** and state that your views are your own to make it clear that you are not speaking on behalf of the company.
* Exercise extreme caution when making declarations or promises towards customers and other stakeholders on social media channels. As a guideline, avoid commenting on matters that fall outside of your role.
* When operating official accounts you must avoid deleting or ignoring comments with genuine feedback or remarks. These comments are an opportunity to connect with our stakeholders and should be proactively addressed. In the event that a comment, question, or concern falls outside of your area of expertise please leverage relevant internal contacts for assistance.
* Employees must be honest and accurate in their representation of **<<COMPANY>>.** In the event that you post misinformation about **<<COMPANY>>** or post misinformation on **<<COMPANY>>** social media accounts you must correct or remove the content in a timely manner. Such corrections may require a correction notice depending on the context.
* Employees are not permitted to create new accounts that directly represent **<<COMPANY>>** without prior approval from **<<CONTACT>>.**

### Information Security Responsibilities

* When using personal or corporate social media accounts, employees must maintain the confidentiality of trade secrets and private or confidential information. This includes refraining from making company-related announcements before their official announcement period and posting internal reports, policies, procedures or other confidential internal documents.
* With regards to financial disclosure laws employees must not provide confidential company information to others with the intention of informing the purchase or sale of stocks or securities.
* Wherever possible, social media account managers should avoid sharing passwords for company-owned accounts. Social media management tools that allow the addition, limitation, and revocation of account access should be used instead.
* Company-provided email addresses must not be used to create personal accounts; such misuse increases the risk of accounts becoming compromised. Compromised accounts increase the risk of fraud, data theft, and the further compromise of **<<COMPANY>>**’s systems.

### Other Best Practices

* For the most effective resolution, employees are strongly encouraged to settle workplace grievances internally and avoid postings on social media about workplace issues.
* Employees should be aware that any of the information or communications posted on their social media can potentially be accessed by their colleagues, managers, competitors, law enforcement agencies, and those that may be outside of the employee’s trusted network.
* It is strongly recommended that employees receive consent before referring to or posting images of current or former employees, vendors, suppliers, and customers.

### Intellectual Property Rights & Account Ownership

* All accounts that are created for the purpose of representing **<<COMPANY>>** are the sole and exclusive property of the company. This includes all followers, messages, postings, and other content associated with the accounts.
* All personal accounts will remain the property of the employee. **<<COMPANY>>** will **never** request the usernames and passwords for employee-owned social media accounts and any such requests must be reported to **<<CONTACT>>** for corrective actions.
* While employees are encouraged to positively represent **<<COMPANY>>** on their personal social media accounts, said accounts must not be used to officially represent the company without prior approval.
* When sharing content on **<<COMPANY>>’s** official social media accounts, employees must exercise due diligence in respecting the intellectual property rights of others. All content that is shared to official accounts must respect copyright and intellectual property laws.
* Depending on the context of non-original content and relevant copyright and intellectual property laws, all content must be either free of copyrights, be shared with the explicit permission of the copyright owner, or shared with proper attribution to the copyright owner. It’s critical to note that attribution alone is often insufficient.

## Enforcement

* While in the vast majority of instances **<<COMPANY>>** does not have the authority or desire to dictate what its employees post and share on social media sites, egregious conduct that has the potential to harm the reputation and/or performance of **<<COMPANY>>,** its customers, employees, and other stakeholders may be subject to disciplinary action up to and including termination or legal action.
* **<<COMPANY>>** reserves the right to monitor the online activities of its employees as well as any online communications made using company resources. This monitoring may include, but is not limited to, social listening tools, using monitoring tools on company-owned devices and networks, anonymous reports from concerned stakeholders, and the hiring of third-party companies.
* Wherever possible all grievances will be resolved internally without resorting to legal actions. Extreme cases of misconduct such as intellectual property infringement claims, the neglectful or malicious breach of one’s information security responsibilities, and the dissemination of obscene or hateful materials may require legal action.

## Points of Contact

If you have any comments, questions, or concerns about this social media policy please direct them to the relevant point of contact.

* **<<CONTACTS FOR HUMAN RESOURCES, MEDIA, LEGAL, AND OTHER RELEVANT DEPARTMENTS>>**

**<<END OF TEMPLATE>>**

## More Resources From CurrentWare

### [Internet Use Policy Template](https://www.currentware.com/blog/internet-usage-policy/)

This internet acceptable use policy sample will serve as the cornerstone for communicating the expected use of technology in the workplace. With this policy you will set guidelines for user productivity, personal conduct, and information security.

### [Work From Home Policy Template](https://www.currentware.com/blog/work-from-home-policy/)

A work from home policy is an essential remote workforce management tool. To get you started, this free work from home policy template is ready to be downloaded and tailored to your company’s needs.

### [Workplace Monitoring Policy Template](https://www.currentware.com/blog/workplace-monitoring-policy-template/)

A **workplace monitoring policy**—also known as an employee monitoring policy or employee privacy policy—is a type of privacy policy that establishes privacy expectations when monitoring employees in the workplace.

### [CurrentWare's Internet Filtering & Monitoring Software **(Free Trial)**](https://www.currentware.com/solutions/workplace-internet-filtering-monitoring-software/)

With CurrentWare’s workplace internet filtering and monitoring software you can prevent employee internet abuse. Restrict access to undesirable websites with custom software-enforced internet use policies for each group of users or computers. Monitor employee internet use to verify that social media and other sites are not becoming a distraction.

## [About CurrentWare](https://www.currentware.com/about-currentware/)

CurrentWare is a software company that provides a suite of solutions for computer monitoring, web content filtering, data loss prevention, and remote PC power management.

[CurrentWare’s solutions](https://www.currentware.com/products/currentware-suite/) are adopted by a wide array of government and private organizations including schools, hospitals, libraries, and for-profit businesses. CurrentWare customers improve their user productivity, data security, and business intelligence with advanced awareness and control over how technology is used in their organization.

At CurrentWare, our mission is to help businesses increase employee productivity and data security. We achieve this through our commitment to providing user friendly solutions with high quality customer service.