# Social Media Acceptable Use Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies both within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures both within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The use of social media within [Company Name] for business purposes is increasing and the need for social media standards is growing. The purpose of this policy is to set employee expectations and establish standards for appropriate use of social media.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions i.e. those people, elements or situations that are not covered by this policy or where special consideration may be made.

This policy applies to all employees [check current definition of “employee” and list any other types of employees if necessary, e.g. contractors, casual workers, etc.] who use social media in the course of their duties.

# Definitions

Define any key terms, acronyms or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. All requests for employee use of external social networks must be submitted to IT through the move/add/change (MAC) process and must be pre-approved by [Company Name’s] IT Liaison.
2. [Company Name’s] social media accounts are intended to be used solely for business purposes.

**The following are examples of legitimate business usage of public social media:**

* Building positive brand image.
* Increasing mind share: Social media can reach large audiences at very low monetary cost, giving [Company Name] another medium for promotion, increasing brand awareness.
* Providing customers with more timely and personal service in the medium that they prefer will increase satisfaction.
* Monitoring public opinion on [Company Name], [its products and services, or its competitors].
* Increasing customer retention: Using social media builds affinity and loyalty since customers are engaged using a medium they prefer.
* Creating custom network applications (a.k.a. plug-ins) for product and brand promotion or integration with [Company Name’s] own online services.
* Professional networking, such as maintaining academic contacts or maintaining contacts with members of professional or standards organizations that can lead to prospecting.
* Quickly and efficiently responding to customer service issues. The answer to a problem can be public, making it searchable by other customers that have the same request.
* [List any other legitimate business uses.]

**The following activities are deemed inappropriate uses of social media:**

* Use of social media for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
* Use of social media that in any way violates [Company Name’s] policies, rules, or administrative orders, including, but not limited to, [list any applicable code of conduct policies, etc.].
* Opening attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
* Sharing social media account passwords with another person, or attempting to obtain another person’s social media account password.
* [List any other inappropriate uses.]
1. Use of personal social media accounts and user IDs for company use is prohibited. [All process-driven use of social media shall be managed by social media management platforms (SMMPs). Employees will have accounts on the SMMP to access [Company Name] social media properties and shall not directly access [Company Name’s] social media accounts with the social media services themselves.]

**OR:**  [IT will create a user ID on the targeted social media service using the employee’s corporate email address and will communicate the initial account password to the employee. The employee will receive an account activation email directly from the social media service.]

1. Use of [Company Name] social media user IDs for personal use is prohibited. Examples of prohibited use of [Company Name] User IDs include: downloading and installing plug-ins or helper applications such as those that try to access the company email directory, joining groups using a [Company Name] user ID for personal reasons, or adding personal friends to an employee’s friends list.
2. [If access to public social media sites is currently blocked, this step may be necessary. Special access rights are generally not required for 100% cloud-based SMMPs. Rather, they proxy all communication with social media services through their own cloud.]IT will establish access for any applicable [apps/employees] to the targeted social media site [as required for a SMMP to function], making exceptions in firewall, proxy, or web content filter rules.
3. [Depending on the social media site being used, IT may want to provide a link to the current Terms of Service (TOS) or Terms of Use (TOU) for that network and require employees to acknowledge they have reviewed it.]. [Company Name or Social Media Steering Committee] agrees that they will regularly monitor and moderate activity. It is the responsibility of [Company Name] to monitor activity, as well as to ensure company use of the social media site complies with the service’s TOS or TOU, as applicable. Each social media service maintains its own TOS and TOU.
4. Creation of “groups” within the social network to support business goals is allowed. However, [Company Name] agrees that they will regularly monitor and moderate group activity. It is the responsibility of [Company Name] to monitor *individual* group member activity as well as to ensure company use of the social network complies with the social network’s Terms of Service (TOS) or Terms of Use (TOU), as applicable.
5. [IT must assist [Company Name or Social Media Steering Committee] in establishing initial account management procedures for use of an SMMP or other social tools that aggregate and centrally manage [Company Name’s] social media accounts properties.]
6. In compliance with [Company Name’s] record retention policies, social media content may be retained in the organization’s archives, or as backup copies, even after they are deleted from an employee’s mailbox. The goals of the backup and archiving procedures are to ensure system reliability, prevent document and data loss, comply with regulatory and legal requirements, and supply evidence in the event of litigation.
* Backup copies exist primarily to restore service in case of failure. Archival copies are designed for quick and accurate access for a variety of management and legal needs. Both backups and archives are governed by [Company Name’s] document retention policies. These policies indicate that email must be kept for up to [insert number] years. [Replace with details of retention policy.]

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of access to some or all computing and networking resources and facilities;
2. Disciplinary action according to applicable [Company Name] policies;
3. Termination of employment; and/or
4. Legal action according to applicable laws and contractual agreements.