Pagefreezer

GOVERNMENT SOCIAL MEDIA POLICY GUIDE AND TEMPLATE

Key Considerations for the Implementation of an Effective Social Media Policy

TABLE OF CONTENTS

1. Why You Need a Social Media Policy

Like all businesses and organizations, public entities need to put a policy in place that guides the use of social media platforms, both within the agency and externally. This is important because multiple employees (and departments) will need the authorization to post to accounts and moderate content, and without clear rules and guidelines of what constitutes "acceptable" use, it's all too easy to find yourself in a situation where inappropriate content makes its way online—and the repercussions of that can be significant.

Additionally, it's important to consider what employees will be allowed to post and do on their personal social media accounts. While they should remain free to use social media channels in any way they personally choose, they shouldn't post official communications to private accounts, and they should not make use of company credentials to log into these accounts.

Lastly, it's necessary to set out policies for the external use of social media accounts. In other words, citizens should be able to refer to the document when trying to understand how content is moderated and where—as per public records laws—archives of social media activity can be found.

The aim of this guide is to provide the framework necessary to implement an effective social media policy that governs the use of both official and personal accounts. The two sections below will outline the necessary requirements. The final section—the bulk of this document— will provide a template example that can be used in the creation of a policy. The guide will start off below by looking at policies for the use of official social media accounts.

2. Policy Considerations for Official Account Use

A social media policy should outline the following:

2.1 Acceptable Use of Social Media Platforms

Although it's impossible to anticipate every form of content that will be shared on social media channels, it's necessary to have a broad idea of the sort of content that is unacceptable. For instance, employees will likely not be allowed to share political content or promote commercial endeavors.

2.2 Acceptable Social Media Conduct & Disciplinary Action

In addition to discussing acceptable content, the policy should also outline unacceptable conduct and the steps that will be taken in the case of a violation. For example, it should state that employees are not allowed to use profanity and that they can't share graphic content. Failure to do so would result in a loss of privilege to participate in official social media activities.

2.3 Approval of Accounts

Although multiple members of an agency or department might be allowed to post to social media channels, the approval and registration of new accounts should be more tightly controlled. The policy should indicate which individuals in the organization are allowed to authorize a new account.

2.4 Moderation of Content

It's important to keep in mind that a social media policy is not only for internal users. With this in mind, it should outline how the agency moderates third-party content like comments and replies posted by individuals outside the organization. For example, it should stipulate that any comments containing offensive language or violent threats will be removed.

2.5 Records Retention & The Public Records Act

Like other forms of communication, posts and comments on official government social media channels are governed by public records laws. This means that all account activity—including deletion of content—should be archived and made available upon request. The policy should explain how all content is archived, and how both internal and external users can access this archived data.

3. Policy Considerations for Personal Account Use

A social media policy should outline the following:

3.1 Acceptable Use of Personal Accounts

Organizations must emphasize that employees shouldn't blur the line between professional and personal accounts. Their personal accounts shouldn't be used to conduct official business, and they shouldn't use official agency credentials (emails & passwords) to log into personal accounts.

3.2 Acceptable Conduct

Although employees should be free to use personal accounts as they see fit, they should also be reminded that inappropriate behavior will nevertheless reflect negatively on the agency, so responsible conduct is always encouraged. Ideally, it should be stated in their user bios that all comments and opinions are their own.

4. Sample Policy Template

[See accompanying Sample Policy Template.docx for editable version]

Social Media Policy of [THE ORGANIZATION]

Purpose of Document

This policy document outlines the requirements for acceptable use and behavior surrounding the social media accounts of [THE ORGANIZATION], both for internal and external users.

Social media platforms have become invaluable tools for communicating with large audiences—and the organization encourages the use of social media to communicate with constituents—but it is important to keep in mind that social media posts and comments constitute official communication, so they must align with the larger communication policies and strategies of the organization. It's therefore crucial that this document be used in conjunction with other relevant communication documents.

Acceptable Use of Social Media Platforms

Employees are not automatically allowed to use official social media channels to publish content. Before being furnished with login credentials and allowed to publish, an employee must first receive authorization from [RELEVANT MANAGER OR DEPARTMENT].

All posts and comments should align with the larger communication strategies and policies of the organization, and may need approval before being published. This especially holds true for any information governed by press/media policies.

Only content relevant to the mandate of the organization may be published to social media channels. Employees are not allowed to:

- Make statements that are not endorsed by the larger organization.
- Publish content that is irrelevant to the mandate of the organization.
- Share confidential information.
- Make any commercial endorsements or conduct private business.

Acceptable Use of Personal Accounts

Employees are allowed to have personal social media accounts, but they may not:

- Use these accounts to conduct organization business.
- Publish official statements to personal accounts.
- Make use of official email accounts or login credentials to log into these personal accounts.

Employees are also encouraged to:

- Make their role within the organization clear when choosing to respond to official organization statements/posts on social media channels.
- Place a disclaimer in their user bios emphasizing the fact that all opinions are strictly their own.

Acceptable Social Media Conduct & Disciplinary Action

All communication on official social media channels must remain cordial and professional, and should align with the larger communication policies and practices of the organization. Employees are not allowed to:

- Criticize or attack any individual/organization.
- Make any political statements not sanctioned by the organization.

- Make use of profanity.
- Share obscene material.
- Make use of any form of hate speech.
- Depict or encourage violence and other illegal activities.
- Display sensitive and personal identifying information (PII).
- Promote commercial products/services.
- Post copyrighted material that [THE ORGANIZATION] does not have the right to use.
- Share information that could reasonably be argued to place the public in danger.

This also holds true for employees' online replies to comments made by external users. Regardless of the inappropriate nature of these comments, employees must remain professional and continue to conform to the rules set out above when replying or performing any other action.

Additionally, employees should aim to make all communication as clear and concise as possible. This means maintaining professional standards in terms of grammar and spelling, and avoiding unnecessary acronyms and other jargon.

Any employee who fails to follow these guidelines may lose the privilege of taking part in the organization's social media activities. As with other organization policies and guidelines, extreme infractions may result in more severe disciplinary action.

Acceptable Conduct on Personal Accounts

This document does not attempt to govern employee conduct on personal social media accounts. However, employees are encouraged to keep in mind that they will still be seen as representatives of the organization, even when posting to personal accounts, so any disreputable conduct will reflect badly on the organization.

As mentioned in the section above, employees are encouraged to place disclaimers on personal social media channels stating that all opinions are their own.

Approval of Accounts

The following steps must be followed when a new official social media account is registered:

- The creation of the account must be undertaken/approved by [RELEVANT MANAGER OR DEPARTMENT].
- The account must be managed only through approved tools.
- Those with approval to post to the social media account and manage content must be clearly indicated.
- Only official organization credentials may be used to create and access the account.
- Account login credentials may not be shared with anyone who does not have official authorization to make use of the account.

Moderation of Content

The following section applies to content—such as comments and replies—posted to official social media channels by external users.

Content published to official social media channels—both by internal and external users—is continuously monitored. The organization will not allow content to be posted to official social media channels that:

- Makes use of profanity.
- Contains obscene material.
- Contains any form of hate speech.
- Depicts or encourages violence and other illegal activities.
- Displays sensitive and personal identifying information (PII).
- Promotes commercial products/services.
- Contains partisan political statements.
- Can reasonably be argued to place the public in danger.

Should any content be posted that falls within the categories mentioned above, the organization will endeavor to remove it.

Blocking of Public Access

All official social media accounts are considered to be public forums containing official organization communication, and citizens will therefore not be prevented from accessing the information they contain. While the organization reserves the right to remove inappropriate content, it will refrain from blocking users from viewing and interacting with official accounts.

Records Retention & The Public Records Act

As a public-sector organization, all communication over social media channels are subject to public records laws. As a result, the organization will endeavour to respond to all record requests related to its social media content. To accomplish this, all data related to its social media accounts is collected and archived.

The organization makes use of an archiving and compliance solution provided by Pagefreezer. Leveraging this solution:

- Data is collected in real-time and includes all activity such as posts, comments, likes, private messages, etc. It also includes removed content such as deleted comments and unlikes.
- All media related to content is collected, including photos, videos, live streams/broadcasts, etc.
- All data is digitally signed (SHA-256) and timestamped in order to satisfy legal requirements for submitting digital content as evidence per the Federal Rules of Evidence.
- As per the established retention schedule of the organization, social media records are retained for a period of [.....].
- A public access portal that offers search and live replay of all archived social media content can be found at: [.....].

  Content can also be exported to PDF, if necessary.

About This Document

Due to the varying nature of government organizations and agencies, this document cannot be entirely comprehensive—policy requirements will depend on the size and scope of the particular organization. However, it will hopefully provide a useful framework that can be used to craft a specific policy that meets the needs of the organization.

About Pagefreezer

Pagefreezer is a leading provider of website, social media and enterprise collaboration archiving and compliance solutions to a wide range of industries including finance, legal, telecom, retail, utilities, government, and post-secondary education. Pagefreezer is a SaaS (Software-as-a-Service) application that enables organizations and corporations of all sizes to permanently preserve their website and social media content in evidentiary quality and then access those archives and replay them as if they were still live. Uses for the archived data range from compliance with regulators such as the SEC, FINRA and the FDA to litigation preparedness, evidence capture, call center support and competitive intelligence.

For more information, please visit https://www.pagefreezer.com.