

Model Policy for Social Media for State Government Agencies

Introduction and Definitions

This document serves as a template for Kentucky state agencies who are creating an internal Social Media Policy. Agencies should use this policy to guide them in the appropriate creation, use, management, and deletion of their social media presence while also abiding by all relevant public records laws and regulations.

The term **Agency** appears throughout the model policy to allow for a “find/replace” with your Agency’s name to begin work on your own policy. As needs vary from one government body to another, you will need to customize it further to best fit your needs.

For Kentucky Executive Branch agencies, this policy must be read in conjunction with Commonwealth Office of Technology (COT) policy CIO-061: Social Media Policy, which establishes statewide requirements for secure, compliant, and approved use of social media platforms by public agencies. CIO-061 is authorized under KRS 42.726 and sets minimum standards for access, branding, account protection, and use limitations.

Agency social media accounts should not be used to subvert KRS 61.800 through 61.850 (Open Meetings of Public Agencies).

Additionally, users of agency social media accounts must adhere to the Commonwealth Office of Technology’s Acceptable Use Policy (CIO-060), which governs the responsible and ethical use of state IT resources, including internet access, devices, and publishing platforms.

This final policy must adhere to all terms and provisions of the ENT-301 Acceptable Use and Social Media Guidelines, all of which are a part of and incorporated into CIO-061: Social Media Policy and Acceptable Use Policy (CIO-060).

The Public Records Act (KRS 171.420-171.740) defines public records as, “...documentary materials, **regardless of physical form or characteristics**, which are prepared, owned, used, in the possession of or retained by a public agency.” Social media content that meets this definition must be managed in accordance with all applicable laws and regulations.

Definitions for this Policy:

Content – Posts, comments, messages, and other interactions made to an agency social media site.

Coordinator – Agency employee who manages an agency social media account by posting content and responding to comments. The coordinator may be the agency's Communications Officer.

Contributor – Agency employee who creates content for an agency social media account. There may be multiple Contributors at an agency, or the Contributor and Coordinator may be the same person depending on agency size and needs.

Copyrighted Material – Information and materials protected by Copyright Law. If copyrighted, it may not be publicly circulated without prior authorization from the copyright holder.

- Copyright Law of the United States: <http://copyright.gov/title17/>
- Copyright and Fair Use: <https://ogc.harvard.edu/pages/copyright-and-fair-use>

Social Media – A collection of internet-based tools that integrate technology, social interaction and content creation. These tools facilitate collaboration and information sharing. Web-based communities and hosted services include social media sites, networking sites, video and photo sharing sites, wikis, blogs, virtual worlds, and other online interactions and technologies.

Social Media Team - The organized group who creates content for an agency social media account, reviews public comment, posts on behalf of the Agency, and replies to comments. This group can include regular contributors, IT personnel, graphic designers, and the Agency's records officer.

Add any relevant definitions to your own agency policy.

Agency Policy for Social Media

Table of Contents

Purpose	3
Responsibilities of Coordinators and Contributors.....	4
Account and Password Management.....	4
Terms of Services	5
Copyright and Access Restrictions	5
Disciplinary Action.....	5
Setup, Use, and Oversight	5
Setting up Social Media Accounts/Tools	5
Reviewing Content Before Publication	6
Managing Appropriate and Inappropriate Content	6
Managing Transfer of Social Media Accounts.....	7
Deleting Accounts	7
Site Content.....	7
Content as Public Records	7
Endorsement Disclaimer	8
Resources	8

Purpose

Agency supports the use of agency social media accounts to build relationships that will support the public and promote **agency's** mission. Employees will use appropriate agency social media accounts correctly and efficiently to support the work of the department. Employees will use agency social media accounts to reach the widest possible audience and to maximize transparency regarding the work of **agency**.

Agency will use agency social media accounts to:

- Announce new services/programs
- Post news such as closures, special events, holiday hours, etc.

- Highlight official staff activities
- Serve as a public relations/marketing tool

Responsibilities of Coordinators and Contributors

Coordinators and contributors will be responsible for obtaining approval to use an official agency social media account from their supervisor, and will be responsible for taking any appropriate training, before the creation and use of agency social media accounts. Coordinators and contributors should see that all communication through agency social media accounts remains professional in nature. Coordinators and contributors must not use social media sites for unapproved political purposes, to conduct private commercial transactions, to engage in private business activities, or have personal conversations. When representing **agency** or acting in an official capacity in response to a communication on an agency social media site, coordinators and contributors should only use **agency** accounts and should not offer personal or non-official opinions. No personal accounts may be used to conduct official business, and no official accounts may be used for personal opinions or non-agency content.

Staff may not access or operate personal social media accounts on state-owned computers, tablets, or mobile phones unless explicitly authorized for official duties. All use of state IT resources must comply with CIO-060 and be limited to professional, ethical, and responsible conduct. Content must not solicit political, religious, or illegal causes, nor misrepresent the agency.

Account and Password Management

Coordinators and contributors should:

- Create unique accounts or profiles devoted to business-related use of agency social media accounts which are only used for work-related communication.
- Identify the page as the **agency** or themselves as employees of **agency** and/or their division on the account or profile being used.
- Create unique passwords for each site which are shared with the **agency** social media team and/or Communications team to prevent loss of access to the account.
- Ensure passwords for agency social media accounts meet complexity requirements consistent with COT's enterprise security policy.
- Change account passwords routinely and immediately upon personnel transitions.

When creating **agency** accounts, coordinators should use their government-issued email addresses and/or a shared work email account and their real names, and/or titles. Aliases or made-up persons should not be used.

Do not create personal social media accounts with your official government email address.

Terms of Services

Coordinators and contributors should be aware of the current Terms of Service (TOS) of the platform they are using. If the TOS contradicts agency policy, **agency** should not use that platform.

Agencies may not use social media platforms where the platform's TOS conflict with Commonwealth policies. At this time, use of applications owned by ByteDance Limited (e.g., TikTok) is prohibited, except for approved law enforcement purposes.

Copyright and Access Restrictions

Coordinators and contributors should respect copyright and fair use.

Under no circumstances may agencies release non-public, sensitive, confidential, or personally identifiable information, including Federal Tax Information (FTI), through agency social media accounts. Agencies must also refrain from posting content related to ongoing or potential litigation.

Disciplinary Action

Coordinators and contributors who violate CIO-060 and CIO-061 or other internal policies may be subject to disciplinary action, up to and including dismissal. Staff are responsible for using state IT resources, including agency social media accounts, in accordance with applicable laws and enterprise policies. Unauthorized or negligent use of agency social media accounts that result in the release of sensitive or non-compliant content will be reviewed in accordance with agency HR policy and state information security regulations.

Setup, Use, and Oversight

The **agency's** social media coordinator(s) will have responsibility for oversight of the use of agency social media accounts by any contributors.

Setting up Social Media Accounts/Tools

Social media coordinators will oversee the establishment and maintenance of all business-related social media initiatives by **agency** employees. Requests for use of new agency social media tools will be presented to the Coordinator and/or Social Media Team for approval. The proposal should indicate the platform, how it will be used in relation to **agency** and/or division activities, and benefits of using the particular platform.

Reviewing Content Before Publication

Social media coordinators will review content before it is posted on all business-related agency social media sites and will decide whether it is appropriate. Communication should include no overtly political or religious commentary; no form of profanity or obscenity; no copyright violations; and no confidential information.

The types of content that will not be permitted include but are not limited to:

- Obscene or racist content
- Personal attacks, insults, or threatening language
- Potentially libelous or slanderous statements
- Personal information published without consent
- Comments unrelated to the content of the forum
- Hyperlinks to material that is not directly related to the discussion
- Commercial promotions or spam
- Posts or comments in violation of the copyright, trademark right, or other intellectual property right of any third party

Managing Appropriate and Inappropriate Content

Social media coordinators will manage the posts and comments appearing on all business-related agency social media sites and will not allow inappropriate posts/comments on these sites. Coordinators will review comments, messages, or other interactions which may be inappropriate, offensive, or threatening. When interactions are inconsistent with this policy the posts/comments must be documented (by the agency for open records requests), then they **may** be hidden or deleted from the site. Etiquette may dictate communicating the reason for the deletion to the commenter. **Agency** should maintain a folder of removed content so that it can be produced if needed or disposed of after it has met retention. Comments typically consist of Routine Correspondence from the public to the agency and should be retained for up to 2 years.

Blocking users or accounts should only be applied in extreme circumstances, e.g., a user has been notified that they posted inappropriate content, but they continue to do so. To initiate blocking, the coordinator will present a summary of the problem and make a recommendation to the Social Media Team or leadership staff, who will issue a decision based on the presentation and any other information which may be available. **Agency** should maintain a list of blocked accounts along with the date and reason for the decision. This list should be reviewed regularly by the social media team for audit of blocked accounts.

Agency reserves the right to edit or remove any postings or comments made to **agency**-sponsored sites. **Agency** does not endorse or review content outside the pages created by

agency staff. Users should be aware that third party websites have their own privacy policies and should proceed accordingly.

Managing Transfer of Agency Social Media Accounts

The **agency's** Coordinator(s) and/or Social Media Team should create and implement a process to transfer **agency** social media accounts to prevent orphaned accounts (due to a staff change). To aid in this effort, **agency** social media accounts should not use an individual's email as an account owner, but rather a group or shared address.

When offboarding staff, agencies must ensure the timely removal of access to official agency social media account credentials in accordance with access control procedures and state IT policies. This includes termination of credentials used on any Commonwealth-managed infrastructure or devices, as required by CIO-060.

Agencies must ensure business continuity by maintaining ownership and administrative access to all accounts at the organizational level. This includes updating credentials upon staffing changes and documenting recovery plans for account compromise or loss of access.

Deleting Accounts

Requests for deletion of agency social media accounts should be directed to the Coordinator and/or Social Media Team for approval. Public records that have been created on the agency social media accounts must be appropriately managed per the retention schedules before the account can be deleted.

Site Content

All business-related agency social media accounts should be clearly identified as **agency** accounts through name or title and/or the use of approved logos, photos, or other branding elements. Wherever possible, content posted to agency social media accounts should contain links directing users back to the **agency's** official website for in-depth information, forms, documents or online services necessary to conduct business with **agency**.

Content as Public Records

Communications via agency social media accounts may be public records under KRS 171.410(1) and may be subject to appropriate retention and disposition. Because others might not be aware of public records laws, coordinators should include the following statement on agency social media accounts, if able:

“Communication through agency-related social media is considered a public record under KRS 171.410(1) and will be managed under the terms of KRS 171.410 through 171.740 and 725 KAR Chapter 1.”

Coordinators who receive messages through the private message services offered by social media sites should encourage users to contact them by phone, by an agency email address, or by visiting the **agency**. Private messages received by coordinators should be treated as constituent emails and therefore are public records. Coordinators can choose to turn off comments and messaging on agency social media accounts and use the pages as bulletin boards rather than forums.

Use of agency social media accounts on state-owned devices or networks does not create an expectation of privacy. Per CIO-060, all activity and content are subject to logging, monitoring, and disclosure as needed to enforce compliance.

Questions about managing social media records should be directed to the **agency’s** records officer or the Electronic Records Branch of the Kentucky Department for Libraries and Archives. Written guidelines can be found here:

- [Guidelines for Managing Social Media Records in Kentucky Government](#)

Endorsement Disclaimer

Agency should consider including a disclaimer statement from CIO-061 (Social Media Policy) on each social media site to avoid the appearance of endorsement by the agency.

“Any posting to this page may be subject to disclosure to third parties. Agency reserves the right to address or remove posts or comments at its discretion. Agency has not evaluated and does not endorse any products advertised or opinions expressed on this page.”

Resources

[ENT-301 Acceptable Use and Social Media Guidelines](#)

[CIO-060: Acceptable Use Policy](#)

[CIO-061: Social Media Policy](#)

[Guidelines for Managing Social Media Records in Kentucky Government](#)