	Georgia Technology Authority	
Title:	**Social Media Responsible Use**	
PSG Number:	**SM-25-001**	
Effective Date:	07/01/2025	**Review Date:**
Synopsis:	Establishes common standards when communicating and interacting through social media channels	

PURPOSE

Social media is an essential tool within state government for engaging with the public, sharing information, and promoting transparency. The purpose of this standard is to provide clear guidelines for the responsible use of social media by state government employees and officials. It aims to ensure that social media engagement aligns with the core values of transparency, accountability, and professionalism. The goal is to maintain public trust by promoting ethical behavior, safeguarding sensitive information, and preventing misuse or misrepresentation of government communications. Additionally, it outlines the proper use of social media to protect privacy, ensure security, and comply with legal and regulatory obligations.

SCOPE and AUTHORITY

O.C.G.A 50-25-4(a)(8) – *State Government, Georgia Technology, General Powers*
O.C.G.A 50-25-4(a)(20) - *State Government, Georgia Technology, General Powers*
PM-04-001 – *Information Technology Policies, Standards and Guidelines*
PS-08-005 – *Enterprise Information Security Policy*

TERMS AND DEFINITIONS

Agency - every state department, agency, board, bureau, commission, and authority but shall not include any agency within the judicial or legislative branch of state government, the Georgia Department of Defense, departments headed by elected constitutional officers of the state, or the University System of Georgia and shall also not include any authority statutorily required to effectuate the provisions of Part 4 of Article 9 of Title 11.

Social Media Platform – online application that allows users to publish content and interact with a digital community. A non-exhaustive list of platforms includes Facebook, X, LinkedIn, Instagram, Bluesky, and YouTube.

Social Media Account – identity or profile of a person or organization on a social media platform.

Third-Party Platform – service or software that is managed separately from the main service provider.

STANDARD

All agencies shall adhere to the following requirements when utilizing official social media platform to conduct state business or engage with the public.

- Multi-factor authentication must be enabled on all agency social media platforms to prevent unauthorized use of agency social media accounts. Verification email accounts and phone numbers shall not be tied to an individual. All social media accounts must be accessible to multiple team members to ensure continuous accessibility.
- User roles and permissions shall be actively managed. User permissions and roles shall be checked quarterly and updated to reflect current team roles and access on applicable social media and third-party platforms.
- Agency social media passwords shall be complex, changed quarterly, and stored securely. Password information shall be stored in encrypted third-party applications intended for password storage. Individual users, managing their own login credentials shall also adhere to this requirement.
- Personally Identifiable Information (PII) shall not be shared across social media platforms**.** This includes public responses or private messages. If a follow-up is necessary, direct constituents to a secure means of communication, such as state-run portals or secure forms.
- Agencies shall not block users from official agency social media accounts. Comments may be hidden only if they violate platform or agency social media policies.
- All agency social media posts must be archived by a third-party platform and old posts cannot be deleted until they've been archived and stored according to the appropriate state retention schedule and Georgia State Records Act. Georgia state agencies are required to archive social media posts and cannot delete old posts except through the operation of an approved retention schedule.
- Agencies shall obtain permission in writing before sharing photos of individuals on official agency social media accounts. This shall not include

photos taken in a public place or event where there is not an expectation of privacy or where any person can take a photo of individuals in attendance. Sharing photos of children under the age of 18 shall always require a signed photo release from a parent or guardian. Agencies that provide confidential services to constituents shall never post photos of constituents, regardless of whether they have signed a photo release.

- Agencies shall comply with all photo-credit policies of social media platforms and stock photo providers. Photos taken by others will likely need a credit when posting on social media. Additionally, some stock photo services require a photo credit in certain circumstances. Each stock photo provider's policy will vary. Details can be found in your terms of service.
- Agencies shall stay up to date on Federal Trade Commission (FTC) regulations and guidelines**.** The Federal Trade Commission regulates social media advertising, native advertising, and influencer campaigns. These guidelines and regulations are regularly updated. Violators face penalties and large fines, regardless of whether they were aware of the regulations. Even if the agency does not plan to advertise or use influencers, those responsible for agency social media management shall stay up to date on regulations and guidelines.
- **Social media content, like website content, shall be accessible.** This may mean using image descriptions, video captions, and not putting important information in a graphic.
- Agencies shall not create social media accounts or utilize any software deemed as prohibited under enterprise standard Prohibited Software & Services SS-22-002

RELATED ENTERPRISE POLICIES, STANDARDS AND GUIDELINES

Prohibited Software and Services SS-22-002
Password Security SS-08-007
Appropriate Use and Monitoring SS-08-001
Social Media Guidelines GM-11-002
Digital Accessibility SM-19-002