



New York State Information Technology Policy	No: NYS-P11-001
IT Policy: Use of Social Media Technology	Updated: 12/14/2022
	Issued By: NYS Office of Information Technology Services Owner: Communications & Public Information Office

1.0 Purpose and Benefits

In a world where social media has become a primary source of news and information, it is important that New York State (NYS) maintains a standard social media use policy. The purposes of this policy are to:

- Encourage NYS government entities to permit the responsible use of social media by their employees as part of their official duties;
- Establish minimum requirements for the proper use of social media by NYS government entities and their workforce in a professional capacity; and
- Promote transparency of NYS government, enabling citizens to hold their government accountable on its actions and processes through social media.

For purposes of this policy, the term “social media” typically refers to forms of electronic communication (such as websites and applications for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos).

2.0 Authority

Sections 103(10) and 103(11) of the State Technology Law provide the NYS Office of Information Technology Services (ITS) with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117¹*, issued January 2002, provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information

¹ All references to Executive Order 117 refer to that which was originally issued by Governor George E. Pataki on January 28, 2002 and continued by Executive Order 5 issued by Governor Eliot Spitzer on January 1, 2007, Executive Order 9 issued by Governor David A. Patterson on June 18, 2008, Executive Order 2 issued by Governor Andrew M. Cuomo on January 1, 2011 and Executive Order 6 issued by Governor Kathy Hochul on October 8, 2021.

technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in [NYS ITS Policy NYS-P08-002, Authority to Establish State Enterprise Information Technology \(IT\) Policy, Standards and Guidelines.](#)

3.0 Scope

This policy applies to all “State Entities” (SE), defined as “State Government” entities as defined in *Executive Order 117*, issued January 2002, or “State Agencies” as defined in *Section 101 of the State Technology Law*. This includes their employees and all third parties (such as local governments, consultants, vendors, and contractors) that use or access any IT resource for which the SE has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE. While an SE may adopt a different policy, it must include the requirements set forth in this one.

This policy applies to the official use of social media by an SE and duly authorized SE employees using social media in their official capacities and on behalf of their employing SE. This policy does not apply to an employee’s personal social media account.

4.0 Information Statement

SEs are encouraged to use social media tools to further their missions and engage and inform their constituencies. This policy sets forth the rules and expectations of SEs when using social media.

4.1 SE Use of Social Media

SEs may use social media to further their mission and engage the public. SEs use public-facing social media sites to communicate, inform, and engage the public and promote transparency. The use of private internal social media technologies may also be used by SEs as a business tool to increase collaboration, participation and improved operational efficiencies among the State workforce.

Accounts used to manage the SE’s social media presence are privileged accounts and must be treated as such. These accounts are for official use only and must not be used for personal use. Passwords of privileged accounts must follow NYS-S14-006 – Authentication Tokens Standard, Section 4.2.1 & Table 3: Memorized Secret Token minimum requirements, be unique on each site, and must not be the same as passwords used to access other SE IT resources.

4.1.1 SE Social Media Sites

The decision to create and/or discontinue an SE social media site is the sole responsibility of the SE. SEs must designate an individual to administer their social media site, which could be the SE’s Public Information Officer, Digital Information Officer, or another SE employee whose official duties align with administering a social media site. The SE, and its designated social media site administrators, responsibilities for administering the SE’s social media site include, but are not limited to the following:

- securely maintaining the site location and access rights associated with such sites;
- following the New York State Information Technology Policy, [NYS-P10-001, Advertisements, Endorsements and Sponsorships on State Entity Websites](#);
- and
- complying with records retention and archival requirements when discontinuing use of a social media site pursuant to Subdivision 11, Section 57.05 of the Arts and Cultural Affairs Law and 8 NYCRR Part 188.

4.1.2 Content

Only authorized personnel acting in their official capacity may communicate on public SE social media sites on behalf of the SE, and may do so only pursuant to an established content approval process. Personnel are authorized when approved by the SE's Executive management (see [Section 4.2](#)). Content posted on any SE social media site (whether public or internal-facing) must comply with all applicable Federal and State laws, regulations, and policies as well as any terms of use and terms of service applicable to the social media site being used. All SE posts shall be consistent with the SE's social media use disclaimer (see [Section 4.1.3](#) below for further discussion of social media use disclaimers). The SE, with the advice of the SE's legal counsel, should oversee content management of social media sites.

4.1.3 Social Media Use Disclaimer

A "Social Media Use Disclaimer" outlines the expectations of all those using a specific social media technology, whether a member of the State workforce or an external user. For example, many social media tools generate advertisements for third party websites and applications as a source of revenue. SEs must develop and post or link to a disclaimer in a prominent location on each of its social media web pages. All disclaimers must be approved by the SE's legal counsel prior to being posted. The following is an example of a social media disclaimer:

Statewide Social Media Use Disclaimer

Thank you for visiting [AGENCY] on [SITE]. New York State agencies' social media sites are hosted by third-party platforms such as Facebook, Instagram, and X (formerly known as Twitter), which maintain their own terms of service (TOS), terms of use, privacy policies or other rules governing the use of these sites. Information (e.g., photos, videos, graphics, messages, etc.) you share with or post to New York State agencies' social media sites may be used by the owners of the host site for their own purposes pursuant to their TOS. For more information, consult the host website's TOS.

New York State may also host its own social media sites, whose site-specific TOS govern your use of those sites. You agree that any information you post on a New York State social media site is irrevocably and permanently licensed to New York State and may be treated by the State as public information subject to disclosure to third parties and to records retention requirements. If a copyright is indicated on a video, photo, graphic or other material, permission to use the material must be obtained from the original source of the material prior to posting and you must provide appropriate credit to the source as required by law and/or regulation. You

acknowledge that the [AGENCY] may prohibit or remove comments or posts that, in the [AGENCY'S] judgment, violate State and/or Federal law or the [AGENCY'S] applicable terms of use. In addition, the [AGENCY] can prohibit commercial endorsements.

The opinions and beliefs expressed by users on this site are those of the users and do not necessarily reflect the views or opinions of [AGENCY]. Comments posted on this site are not considered formal public comment, legal notice, or a request for records, and are not promised or guaranteed to be accurate, current, or complete. Such comments will not be acknowledged. **If your comment concerns an emergency or criminal matter, please contact 9-1-1 for immediate assistance.** If your comment concerns fraud or governmental misconduct, you should contact the New York State Inspector General at <https://ig.ny.gov/form/complaint-form-long>. [AGENCY] assumes no responsibility for and expressly disclaims responsibility for updating this site to keep information current or to ensure the accuracy or completeness of any posted information. New York State is not required to preserve indefinitely all material posted to its digital outlets. Links or advertisements provided on this website may have been placed there by the social media host site and not the [AGENCY]. Their placement does not constitute an endorsement of the content, viewpoint, accuracy, opinions, policies, products, services, or accessibility of those items by the [AGENCY] or New York State. Once you follow a link to another website from this website, including another website maintained by the State, you are subject to the terms and conditions governing the use of that website.

New York State reserves the right to modify this disclaimer at any time. Continued use of New York State social media pages following the posting of any modification signifies acceptance of such modification.

Questions regarding the New York State social media use disclaimer may be directed to the State government entity's Public Information Officer, Digital Information Officer, Chief Counsel, or other agency designee.

4.2 Use of Social Media by State Workforce Members in their Official Capacities

Duly authorized SE employees may use social media in their official capacities and on behalf of their employing SE. SEs may also authorize employees to use social media technologies to (a) increase collaboration, (b) support greater participation in the SE's operations, and (c) improve operational efficiencies.

Authorized SE employees must adhere to the following rules when using social media technologies through State IT resources and/or when posting to social media sites in their official capacities. Authorized employees must:

- obtain the necessary authorizations from the SE's management and the Public Information Officer, Digital Information Officer, or other agency designee, to communicate on behalf of the entity.
- abide by all applicable policies, terms of use, and work rules including the [Acceptable Use of Information Technology Resources Policy](#), regarding the use of the Internet and information technology resources. The use of social media tools

on State IT resources will be monitored by the same method as defined in those policies and work rules.

- not post personal, private, sensitive, confidential, proprietary, deliberative or otherwise restricted information.
- be transparent when participating in any online community and speaking on behalf of the SE by disclosing their identity and affiliation with the SE.
- communicate in a professional manner.
- abide by copyright and other applicable laws. Comments and posts may be permanently available and open to being republished in other media. Libel, defamation, copyright, and data protection laws apply to postings on social media websites.
- obtain permission before publishing photographs, videos or quotes of others.

4.3 Legal Issues

The legal issues regarding the use of social media may differ across SEs. Therefore, before utilizing social media, SEs should consult with their legal counsel and other relevant parties to review the legal issues relevant to their organization. Specifically, SEs must ensure that their technology tools comply with: privacy laws; applicable New York State information technology policies and standards (see section 9.0 below); records retention and archival requirements, where applicable; Freedom of Information policies and laws; requirements of Federal law (including but not limited to the First Amendment of the Constitution of the United States); the Hatch Act and/or New York State Civil Service Law Section 107, and any subsequent amendments, as well as any other applicable state and federal laws, rules, and regulations; copyrights; and Terms of Service or Use. SEs should also consult with legal counsel to evaluate whether posts or content that a user provides are subject to removal from a social media site before removing them.

4.4 Mitigation of Security Risks

For successful integration of social media into a SE's operation, the entity's information and systems must be secured against malicious activity. Users must be aware that the use of social media within the organization poses risks that can be mitigated but never fully eliminated. SEs should review the [NYS Information Security Policy](#) to help mitigate such risks.

If available on the platform, SE's must use the strongest multifactor authentication possible to secure their social media account. The preferred methods for implementation of multifactor authentication here are in the following order of precedence: security key; app based one-time password or push notification; =SMS based one-time password.

4.5 Personal Use of Social Media

State employees may share personal views and express themselves as private citizens on social media, but such personal use must make clear that it is not an official act of the employee's SE or New York State. In addition, State employees must not share any confidential, private, or sensitive information pertaining to their SE, other employees, or job activities.

Users should be sensitive to the fact that information posted on social media sites clearly reflects on the individual and may also reflect on the individual's professional life. Consequently, users should use discretion when posting information on these sites and be conscious of the potential perceptions of and responses to the information. It is important to remember that once information is posted on a social media site, it can be captured and used in ways not originally intended. It is nearly impossible to retract, as it often lives on in copies, archives, backups, and memory cache.

Users should carefully consider whether to post information about their employment on personal social media sites, including which SE they work for and their job title, as such information could be used for purposes of committing fraud, identity theft, phishing, or other cyber exploits.

Users should follow best practices when using social media in a personal capacity, including the following:

- Be familiar with your SE's policy on the use of any images, logos or information related to the performance of official duties or as a result of State employment.
- Respect the privacy of your State colleagues and do not post any identifying information of any staff without permission (including, but not limited to, names, addresses, photos, videos, email addresses, and phone numbers). Users may be held liable for comments posted on social media sites.
- If a personal email, posting, or other electronic message could be construed to be an official communication, a disclaimer is strongly recommended, such as, "The views and opinions expressed are those of the author and are not authorized by and do not necessarily reflect those of [your Agency] or the State of New York."
- Ensure the passwords used for your personal social media sites are different from those used on SE IT equipment and resources in order to prevent unauthorized access to SE equipment and IT resources if the personal password is compromised.
- Immediately consult your SE's information security officer/designated security representative for assistance in the event you suspect your personal social media account has been compromised in a way that may impact your technology use in your official capacity.
- If available on the platform, use the strongest multifactor authentication possible to secure your social media account as described in section 4.4.

Review your privacy and security settings and be aware of who is able to view your information and posts.

5.0 Compliance

This policy shall take effect upon publication. Compliance is required with all ITS policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is required.

Any violation of this policy may subject the user to disciplinary action, civil penalties, and/or criminal prosecution. The SE will review alleged violations of this policy on a case-by-case basis and pursue recourse, as appropriate.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in <http://www.its.ny.gov/glossary>.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Communications & Public Information Office
Reference: NYS-P11-001
NYS Office of Information Technology Services
State Capitol, ESP, P.O. Box 2062
Albany, NY 12220
Telephone: (518) 402-3899
Email: communications.office@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: <https://its.ny.gov/policies>

8.0 Revision History

This policy should be reviewed consistent with the requirements set forth in [NYS-P08-002 Authority to Establish State Enterprise Information Technology \(IT\) Policy, Standards and Guidelines](#).

Date	Description of Change	Reviewer
10/20/2011	Original Policy Release	OFT/CIO
09/12/2012	Formatting and Branding Updates	OFT/CIO
07/28/2014	Updated Policy	Public Information Office
10/19/2016	Formatting and Branding Updates	Public Information Office
08/14/2018	Updated policy	Web NY Tim Crommie

12/14/2022	Updated policy. Added social media section from NYS-P14-001 Acceptable Use of Information Technology Resources.	Communications and Public Information
------------	---	---------------------------------------

9.0 Related Documents

[NYS-P14-001 Acceptable Use of Information Technology Resources Policy](#)

[NYS-P10-001 Advertisements, Endorsement and Sponsorships on State Entity Websites](#)

[NYS-P03-002 Information Security Policy](#)

[NYS-P20-001 Digital Identity Policy](#)

[NYS-S20-001 Digital Identity Standard](#)

[NYS-S14-005 Security Logging Standard](#)

[NYS-S14-006 Authentication Tokens Standard](#)

[NYS-S14-002 Information Classification Standard](#)