

<p><b>New York State Information Technology Policy</b></p>	<p><b>No:</b> NYS-P11-001</p>
<p><b>IT Policy:</b></p> <p><b>Social Media</b></p>	<p><b>Updated:</b> 11/14/2012</p> <p><b>Issued By:</b> NYS ITS State Chief Information Officer Director Office of IT Services</p> <p><b>Policy Owner:</b> Empire 2.0 Web Services</p>

## 1.0 Purpose and Benefits of the Policy

---

More people than ever are using social media technologies to create, connect, and collaborate online. The term social media is commonly associated with web applications that facilitate interactive information sharing, interoperability, user-centered design, and collaboration on the World Wide Web.

The purpose of this policy is to:

- Encourage state government entities to permit the responsible use of social media by its employees;
- Establish the minimum requirements for the use of social media in New York State government; and
- Help make New York State government more accountable and transparent to citizens.

There are many benefits to using social media technologies in government. Social media tools redefine the relationships between State governmental entities and the public. They improve government transparency, increase collaboration, encourage greater citizen participation, and improve operational efficiency.

Social networking tools such as blogs and wikis help humanize government as well as facilitate and encourage discussion on public policy issues. Multimedia and video sharing tools inform and engage the public about important issues without high maintenance or bandwidth costs. Tools such as mashups allow citizens to view multiple types of publically available data via a web browser.

## 2.0 Enterprise IT Policy Statement

---

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of the NYS Office for Technology, the authority to oversee, direct and coordinate the establishment of information 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 \(IT\) Policy, Standards and Guidelines](#).

## 3.0 Scope of the Policy

---

This policy applies to all “State government entities,” as defined in NYS Executive Order 117.

## 4.0 Policy Statement

---

Using social media technologies can help State government entities engage citizens and make government more open and transparent. New York State government entities are highly encouraged to use social media tools to enhance their mission and engage their constituencies. By following agency expectations for the responsible use of social media, State workforce members should be allowed to access social media for professional or personal use while agencies implement accountable social media usage permissions as set forth below.

### 4.1 Agency Use of Social Media Tools

#### 4.1.1 State Government Entity Social Media Sites

The creation, maintenance and destruction of State government entity social media sites is the sole responsibility of the State government entity. The State government entity Public Information Officer or other designee must keep on file a list of official State government entity social media sites and the associated URLs.

#### Content

When using social media sites, only users authorized by the Public Information Officer or other designee may post on behalf of the State government entity. Content posted on State government entity social media sites must comply with all applicable Federal and State laws, regulations and policies. State government entities are required to create a moderation process for all user generated content (i.e., comments, file uploads, etc). State government entities may disable features on social media sites that allow users to post content such as comments, videos, or other types of shared files.

## **Terms of Participation Statement**

A “Terms of Participation” statement outlines the expectations of the users and the agency when using social media technologies. All State government entity social media sites must prominently display or link to, a Terms of Participation statement that includes at a minimum:

- An outline for acceptable user behavior which includes at a minimum, provisions against the following items:
  - Advertising for private or political purposes;
  - Harassment and defamation;
  - Pornographic content;
  - Encouragement of illegal activity; and
  - Sharing of confidential, proprietary or otherwise restricted information.
- Description of the moderation techniques used by the State government entity (i.e., reviewing comments before they appear publically on the site).
- Consequences for violating the Terms of Participation.
- Contact information for questions regarding the use of the site.

## **Example Terms of Participation Statement**

[AGENCY] welcomes and encourages you to participate in the discussion on [SITE]. By contributing to this site, you agree not to post any content that contains advertising for private or political purposes, harassing or defaming images or language, pornographic content, encouragement of illegal activity and the sharing of confidential, proprietary or otherwise restricted information. To keep the discussion open and relevant, all content on this site is moderated by [AGENCY] staff after it is submitted by a user. [AGENCY] reserves the right to delete any content and block or remove any users that violate the Terms of Participation. If you have any questions about the Terms of Participation for this site, please contact [AGENCY] at [CONTACT INFORMATION].

## **Disclaimer**

Many social media tools generate advertisements for third party websites and applications as a source of revenue. To safeguard against potential liability issues, State government entities must develop and post a disclaimer in a prominent location on each branded social media web page that contains these advertisements. All disclaimers must be approved by the State government entity’s legal staff before being posted. See below for an example of a social media disclaimer:

## **Example Disclaimer**

Thank you for visiting [AGENCY] on [SITE]. The opinions and beliefs expressed 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 and are not promised or guaranteed to be accurate, current, or complete. [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. Links or advertisements provided on this website may have been placed there by the social media provider 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. Once you follow a link to another website from this website, including one maintained by the State, you are subject to the terms and conditions of that website.

## **4.2 Use of Social Media by State Workforce Members**

### **4.2.1. Use of Social Media by State Workforce Members in Their Official Capacities**

If a State government entity permits use of social media technologies by State workforce members in their capacities as members of the State workforce, at a minimum, all State workforce members must adhere to the following rules when using such technologies on State government entity IT resources and/or in their capacities as a State Workforce member:

- Abide by all applicable policies and work rules regarding the use of the Internet when using social media tools for business and personal use. The use of social media tools on State government entity IT resources will be monitored by the same method as defined in those policies and work rules.
- Are responsible for all of their online activities that are: conducted with a State government entity e-mail address; can be traced to a State government entity's domain; and/or use State government entity resources.
- Must not discuss or post confidential, proprietary or otherwise restricted information.
- When speaking on behalf of the State government entity, users must be transparent when participating in any online community. They should disclose their identity and affiliation with the State government entity.
- Communicate in a professional manner.
- Abide by copyright and other applicable laws. Participation online results in a user's comments being permanently available and open to being republished in other media. Users should be aware that libel, defamation, copyright and data protection laws apply.
- When communicating on behalf of the State government entity, State workforce members must obtain the necessary authorizations by management and the Public Information Officer, or other designee, as appropriate.
- Must obtain permission before publishing photographs, videos or quotes of others.
- When not representing the State government entity, State workforce members who publish personal or professional opinions must not invoke their State government entity title. In such cases, users must use a disclaimer such as the following where technically feasible: "The postings on this site are my own and do not represent the position, strategy or opinion of (the State government entity)."

#### **4.2.2. Use of Social Media by State Workforce Members in Their Personal Capacities**

To the extent State workforce members use social media in their personal capacities as private citizens, the following requirements apply. Such use must not substantially interfere with the operation of the State or a State government entity(ies), including not violating acceptable use or other policies or laws, such as laws or policies requiring confidentiality. (See, e.g., ITS' Empire 2.0 Legal Tool Kit, Social Media - Legal Issues for Agencies to Consider, available at [http://www.empire-20.ny.gov/legal\\_toolkit](http://www.empire-20.ny.gov/legal_toolkit)).

Notwithstanding the above, nothing in this section is meant to imply any restriction or diminishment of employee rights to appropriately engage in protected concerted activity under law.

#### **4.3 Legal Issues**

The legal issues regarding the use of social media may differ across State governmental entities. Therefore, before the implementation of social media technologies, State government entities should be aware of the legal issues that apply to their organization. Specifically, State government entities need to make sure that the tools they use do not violate any privacy laws, New York State information technology and records policies and laws, copyrights, and Terms of Use policies. Guidance regarding the legal implications of using social media in New York State government can be found in the New York State Center of Excellence Legal 2-Kit ([http://www.empire-20.ny.gov/legal\\_toolkit](http://www.empire-20.ny.gov/legal_toolkit)).

Examples of the topics found in the New York State Center of Excellence Legal 2-Kit include information on the applicability of the Freedom of Information Law (FOIL), Open Meetings Laws and Record Retention/Disposition laws when using social media. The 2-Kit also includes references to tools that may assist New York State Government entities to address these topics.

#### **4.4 Security Risks**

For successful integration of social media into an organization's operations, it is important that there is special consideration given to securing the organization's information and systems from malicious activity. State government entities who engage in the use of social media must at a minimum:

- **Create a Process for Enabling the Use of Social Media Sites**

New York State government entities must create a process for enabling the use of social media tools and other agency blocked websites by State employees and contractors. The process must include at a minimum:

- The submission of a business case prior to the implementation of the tool(s) or access to the site(s). The business case should include at a minimum:

- A risk assessment (including risk mitigation techniques) in the following areas:
    - Employee productivity;
    - Security of State government entity IT assets; and
    - Reputational risk to the State government entity and the State
- Approval from the State agency Commissioner or State agency Chief Information Officer, or designee.
- Notification to the State government entity Public Information Officer (PIO) or other designee.

- **Ensure the Appropriate Policies are in Place**

Based on the results of the risk assessment, security policies may need to be created or updated to extend the coverage of existing policies as they relate to protecting information, assets, and reputation in a Web 2.0 environment. Policies must establish clear expectations for user behavior, both personal and professional, and address information confidentiality, integrity, and availability when accessing data or distributing proprietary information.<sup>1</sup>

Additionally, in accordance with [NYS CSCIC PS08-001 Information Classification and Control](#), it is the responsibility of the State government entity to appropriately classify any information posted on social media sites. To avoid issues with records retention policies and laws, it is recommended that State government entities develop policies that restrict the posting of all non-publicly available information on public social media sites.

It is also recommended that State government entities should “be proactive to ensure that publically vital content remains accessible, and to ensure that any subset of materials which may be subject to records retention laws is treated appropriately.”<sup>2</sup>

All policies must be accessible, available, easy to understand, and communicated to all workforce members.

- **Properly Train Workforce Members**

Training is a key component in establishing and maintaining a secure social media experience. Informed administrators and users are the best defense against social media related risks to a State government entity’s assets. Workforce training should be used to communicate organizational policies as well as educate users on how to identify and defend against potential attacks. Unique considerations resulting from the use of social media technologies should be incorporated into existing employee training or specialized training created and required for site administrators and anyone that is approved to communicate on behalf of the State government entity.

---

<sup>1</sup> “Guidelines for Secure Use of Social Media by Federal Departments and Agencies” ISO Council  
<http://management.energy.gov/documents/SecureSocialMedia.pdf>

<sup>2</sup> State of New York. *Social Media - Legal Issues for Agencies to Consider*. Albany: CIO/OFT, 2010. Web. 30 Mar 2011. <[http://www.empire-20.ny.gov/legal\\_toolkit](http://www.empire-20.ny.gov/legal_toolkit)>

- **Implement Procedural and Technical Controls**

In addition to policy compliance and training, securing information systems from malicious activity can be accomplished by following secure procedures and implementing technical controls. The following controls identify a minimum a State government entity must implement when establishing a social media presence:

- **Use Secure Site Administration**

All administration of a social media technology must be executed using a secure connection if it is supported by the tool. This is typically denoted by the https protocol prefix in the site's URL.

- **Use Unique Usernames for Site Administration**

Unique usernames will help ensure any modifications to the site, intentional or unintentional, can be attributed to a single user.

- **Use Strong Passwords**

Externally hosted social media sites may not require strong passwords. The criteria for strong passwords should be defined in an organizational policy. This will reduce the likelihood of a hijacked account and unauthorized use and modification of your site. More information on strong password can be found in [NYS P03-002 V3.4 Information Security Policy](#).

- **Log Content Changes**

Content logging must be enabled for any action that results in an alteration of content. In the event of an unauthorized alteration, this will allow an action to be traced to a unique username and a determination can be made if the alteration was intentional, unintentional, or the result of a compromised account.

- **Use Non-Privileged Accounts for Web Access**

In the event a user is exposed to a malware installation, an account with limited privileges may prevent a successful installation.

- **Moderate All Posts**

Moderating content will allow for the detection of malicious links and/or inappropriate material. As part of your content moderation procedures, evaluate shortened URL destinations. The full destination URLs can be revealed using browser add-ons or by entering the shortened URL into a free service. Link destinations must also be scanned for malicious behavior prior to posting.

- **Use Current Systems, Browsers and Browser Plug-ins**

Using current patches for systems will reduce the risk to your state assets by eliminating known vulnerabilities.

- **Provide Content Screening**

When accessing a social media site from a State government entity facility, force all traffic through a secure gateway or other content screening solution. Forcing all traffic through a secure gateway or other content screening solution can prevent a user from accessing malicious content or prevent malware from reaching the end user system.

- **Use Current Virus Definitions**

Current virus definitions will help ensure that malware which has been successfully installed on the user's system does not persist on the system.

- **Perform Backups Regularly**

Regular backups will ensure a site can be restored to a working state in the event a compromise allowed for unauthorized modification of the site.

## 5.0 Policy Compliance

---

This policy shall take effect upon publication. The Enterprise Strategy and Acquisition Services Unit shall review the policy at least once every two years to ensure relevancy. The Enterprise Strategy and Acquisitions Office may also assess agency compliance with this policy. To accomplish this assessment, ITS may issue, from time to time, requests for information to covered agencies, which will be used to develop any reporting requirements as may be requested by the NYS Chief Information Officer, the Executive Chamber or Legislative entities.

## 6.0 Definitions of Key Terms

---

A complete listing of defined terms for NYS Information Technology Policies, Standards, and Best Practice Guidelines is available in the "NYS Information Technology Policies, Standards, and Best Practice Guidelines Glossary (<http://www.its.ny.gov/policy/glossary.htm>)."

**Social Media** is media that is created to be shared freely across different web publishing platforms.

## 7.0 Contact Information

---

Submit all inquiries and requests for future enhancements regarding this policy to:

**Policy Owner**  
**Attention: Empire 2.0 Web Services**  
**New York State Office of Information Technology Services**  
**State Capitol, ESP, P.O. Box 2062**

## Albany, NY 12220

Questions may also be directed to your ITS Customer Relations Manager at:  
[Customer.Relations@cio.ny.gov](mailto:Customer.Relations@cio.ny.gov)

The State of New York Enterprise IT Policies may be found at the following website:  
<http://www.its.ny.gov/tables/technologypolicyindex.htm>

## 8.0 Revision History and Review Schedule

---

Date	Description of Change
10/20/2011	Original Policy Release
09/12/2012	Reformatted and updated to reflect current CIO, agency name, logo and style.
11/14/2012	Updated URLs
11/14/2014	Scheduled Policy Review

## 9.0 Related Documents

---

[NYS CSCIC G10-001 Secure Use of Social Media](#)

[NYS CSCIC PS08-001 Information Classification and Control](#)

[NYS CSCIC P03-002 V3.4 Information Security Policy.](#)

[NYS Empire 2.0 Homepage and associated webpages, available at <http://www.empire-20.ny.gov/home>](#)

[NYS-G09-001 Acceptable Use of Information Technology \(IT\) Resources](#)

## **ATTACHMENT A: Agency Guide to Adopting Social Media Tools**

The purpose of this guide is to provide an overview of the recommended steps to successfully implement social media tools in New York State agencies.

### **Step 1: Develop a written plan.**

When looking to adopt social media tools, the first step is to develop a written plan. The plan should include an outline of the objectives, strategies and the key roles and responsibilities of those who may need to contribute to the success of the social media tool. The written plan should also contain clearly defined goals (i.e., promote citizen interaction, disseminate information, reduce marketing costs, etc.), workflows for adding and deleting content, and identify who is responsible for moderating the tool.

### **Step 2: Identify a tool.**

The next step is to identify the proper tool(s) that satisfies the objectives outlined in the written plan. There are numerous Web 2.0 tools available to agencies and each tool has unique functionality. On the surface, many Web 2.0 applications appear to be no-cost or free. However, keep in mind that there may be costs associated with supporting the tool once it is deployed. The selected tool should include features that allow site administrators to moderate content. For more information on the requirements for moderating social media sites see **Section 4.1** of the Social Media Policy.

### **Step 3: Obtain the necessary permissions.**

Before you implement the tool, make sure you obtain the proper approvals in your agency. As outlined in **Section 4.4** of the Social Media Policy, permission from the Agency Commissioner, Chief Information Officer (CIO) or designee must be obtained prior to implementing the social media tool in the agency. Additionally, the Public Information Officer or designee must also be notified before the tool is launched.

### **Step 4: Develop content for the tool(s).**

Use the agency's logo and branding to create a customized look for your social media page. Also add information about the agency including contact information, photos and mission. Remember to post a Terms of Use statement in a prominent location on your page. Additionally, a disclaimer must be included in a prominent location on each agency social media site as outlined in Section 4.1.1 of the Social Media Policy. For more information about the Terms of Use statement, allowable content, and disclaimers on New York State agency social media sites see **Section 4.1.1** of the Social Media Policy.

Be sure to review the Empire 2.0 Center for Excellence website (<http://www.empire-20.ny.gov/>) for tips on how to create and use popular social networking tools such as Facebook and Twitter.

**Step 5: Market the tool.**

Publicizing the use of social media tools is essential to reaching the target audience. The content alone will not draw attention to the site, even though it may be valuable. Agencies can promote social media tools through traditional means such as posting links on the agency website, agency presentations, posters and brochures, press releases and by incorporating them into existing marketing materials.

Additionally, many users may be unfamiliar with using social media tools. Agencies should provide training classes that teach users not only how to administer these tools, but why they are important to support the mission of the agency.