



ANDREW M. CUOMO
Governor

SAMUEL D. ROBERTS
Commissioner

SHEILA J. POOLE
Acting Commissioner

Local Commissioners Memorandum

Section 1

Table with 2 columns: Field (Transmittal, To, Issuing Division/Office, Date, Subject, Contact Person(s), Attachments) and Value (16-LCM-02, Local District Commissioners, OTDA and OCFS Counsel's Office, February 1, 2016, Establishing a Social Media Access Policy for Social Services Districts, OCFS Counsel's Office (518)473-8418, OTDA Counsel's Office (518) 474-9502). Includes an Attachment Available Online checkbox.

Section 2

I. Purpose

This LCM provides local Social Services Districts (SSD) with information and guidance regarding their development of a Social Media Access Policy for use in the SSD. For purposes of this guidance, "Social Media" is defined as any "form[] of electronic communication . . . through which users create online communities to share information, ideas, personal messages, and other content . . . ." Merriam-Webster (http://www.merriam-webster.com/dictionary/socialmedia). This memorandum is intended to convey the broad scope of what a Social Media Access policy in an SSD should include.

Due to the numerous legal implications surrounding the utilization of social media, SSDs must seek the guidance of their attorneys and human resources experts when drafting or modifying their Social Media Access policy. SSDs are reminded of the obligation to comply with the terms of service of all social media sites, as well as the law, rules and regulations of the State of New York and the Federal government, including, but not limited to the Fourth Amendment and Article 1 of the New York State Constitution (particularly as those enumerated sections relate to an individual's right to be secure against unreasonable searches and seizures).

NOTE: This LCM should be read in conjunction with 15-LCM-16, Establishing a Social Media Access Policy for Social Services District Investigators, issued September 29, 2015. Also, please note the NYS Office of Information Technology Services has issued guidance on the Secure Use of Social Media at NYS-G10-001, available at https://www.its.ny.gov/sites/default/files/documents/secure\_use\_of\_social\_media\_guideline\_0.pdf, Social Media Policy at NYS-P11-001, available at https://www.its.ny.gov/sites/default/files/documents/nys-p11-001.pdf, as well as an Acceptable Use of Information Technology (IT) Resources Policy (AUP) at NYS-P14-001, available at https://www.its.ny.gov/sites/default/files/documents/acceptable\_use\_policy\_0.pdf. The scope of

these policies are, however, limited and do not encompass all issues identified for the purposes of this LCM.

Any conflict between the policy language and the current state of relevant law will be decided in favor of the law.

## II. Background

In the past, SSD employees have requested access to social media sites, such as Facebook, through the Human Services Enterprise Network (HSEN). In SSDs not utilizing the HSEN, access was granted by other means controlled by the SSD or county. As personal and professional social media use grows and the SSDs are provided with a means for provisioning staff onto such sites, it is important to highlight the risks and responsibilities involving employees who utilize social media, and create an access policy to assist employees in making responsible decisions about the use of social media.

## III. Essential Elements of A Social Media Access Policy in the SSD

Each SSD providing access to social media sites to employees, as defined below, shall develop and implement a Social Media Access Policy which must provide employees with a comprehensive overview of actions constituting appropriate use when utilizing social media sites regardless of whether or not such access occurs via use of the HSEN. Each SSD shall make their Social Media Access Policy available to OTDA or OCFS upon request. Each Social Media Access Policy must contain the required elements described below:

### a. Definitions

Each Social Media Policy must include definitions of all relevant terms, including but not limited to the following suggested definitions:

**Employee(s)** - Any person employed (whether full-time, part-time or on a seasonal basis) by the SSD, as well as all vendors, contractors and any other person or entity given access to a social media site.

**Equipment** - Any device that has the capability of accessing a social media site, including but not limited to smart phones, laptops, smart watches, iPads, and any other tablets.

**Legitimate Business Purpose** – A purpose that relates to the employee’s official duties An SSD determination that the employee requires access to some or all social media in order for the employee to fulfill his or her job duties.

**Social Media** - Any “form of electronic communication . . . through which users create online communities to share information, ideas, personal messages, and other content . . .” Merriam-Webster (<http://www.merriam-webster.com/dictionary/socialmedia>). Examples include, but are not limited to: blogs, wikis, and social networking sites such as Facebook, LinkedIn, Twitter, Flickr, Instagram, Pinterest, and YouTube. Social media does not include communication using e-mail, fax, or telephone.

b. *Consistency with Acceptable Use Policy*

This section must emphasize that social media policies will be consistent with all applicable state and federal laws, rules, and regulations, as well as SSD policies, including those which may limit the sites to be utilized. Each Social Media Access Policy must require employees to adhere to the New York State Office of Information Technology Services' *Acceptable Use of Information Technology (IT) Resources Policy* (AUP) or any successor policy and any additional policies related to the use of State information technology resources adopted by OTDA, OCFS or the SSD.

c. *Confidentiality Requirements*

This section must set out the confidentiality requirements all employees must follow when utilizing social media sites and the consequences in the event those requirements are not followed. This shall include an employee's responsibility not to violate confidentiality policies, ethics obligations, codes of conduct, and State or Federal laws and regulation. At a minimum, confidential information includes, but is not limited to, any and all client-identifiable information, or any information for which public disclosure is not authorized. Social media may not be used to communicate with applicants or service recipients regarding benefits, program, services or other communication involving official duties, unless otherwise authorized by the SSD to do so. Employees should refer any such outreach from applicants or service recipients to appropriate agency personnel.

d. *Authorized Work-Related Use of Social Media*

This section should include the following essential elements:

i. *Scope & Authorization*

Access to social media must be limited to such sites as may be necessary for the employee to fulfill legitimate business purposes. This section should include how and when social media sites should be accessed.

SSDs must outline the policy for gaining supervisory approval to access social media sites for each program/division. This section must also detail who, within the SSD, has supervisory approval to grant social media access to SSD staff. Furthermore, the SSD must detail who approves access and who administers access.

SSDs must require authorized employees to comply with the Terms of Service of any social media site used. You may refer to the New York State Social Media Policy, found at [www.ny.gov/social-media-policy](http://www.ny.gov/social-media-policy), for further guidance on terms of service of those social media sites.

ii. *Monitoring Responsibilities*

This section must remind employees that they are responsible for the content of their authorized social media accounts. Any use of social media by employees that exceeds the scope of authorization violates the terms of this LCM is strictly prohibited and may result in disciplinary action.

e. *Personal Use*

This section should include the following essential elements:

i. *Prohibited Conduct*

This section must explain that nothing in the SSD policy is intended to impede the rights of employees under the law. Generally, an employee's use of social media is protected under the First Amendment. However, this section should advise SSD staff that any personal use of social media by an employee must not be conducted in a manner that would lead a reader to believe that the employee is speaking for or on behalf of his or her SSD, unless otherwise authorized. Personal social media accounts must not be used for unauthorized SSD business-related purposes. The Prohibited Conduct section should clearly articulate best practices of social media account creation and use, including but not limited to a prohibition on SSD staff utilizing their personal social media accounts for official business and a prohibition on the use of personal accounts to disclose or communicate non-public information acquired through employment, such as legally protected personal information obtained from OTDA and/or OCFS. This section should also remind SSD staff that their use of social media: may not violate any law, regulation, or agency policy; raise suspicion among the public that he or she is likely to be engaged in acts that are a violation of the public's trust; or materially interfere with any employee's execution of his or her duties and responsibilities.

ii. *Use of SSD Title*

SSDs must remind employees that they may use their official title and agency affiliation on their personal social media page for professional identification or biographic data as long as they do not create an impression that they are speaking in an official capacity. Employees must avoid stating or implying that they are communicating in an official capacity in their personal social media activities unless otherwise authorized to do so. If an electronic message could be interpreted as an official communication, then the posting of a disclaimer is strongly recommended. A disclaimer might be stated as follows: "*The views and opinions expressed are those of the author and do not necessarily reflect those of the NYS Office of Temporary and Disability Assistance, the NYS Office of Children and Family Services, the State of New York or [name of SSD].*"

iii. *Use of SSD Equipment*

SSDs should prohibit employees from accessing social media sites in a manner that is inconsistent with any other applicable SSD policies regarding internet use or SSD equipment. This section should remind employees that no expectation of privacy exists in their use of state or SSD equipment, the internet or email, and any such use may be monitored.

iv. *Engaging with Colleagues and Other SSD Stakeholders*

SSDs should acknowledge that employees might engage with colleagues and other SSD stakeholders on their personal social media sites. This section should remind employees to exhibit the same professional and ethical behavior and judgment expected of them in the workplace when using personal social media to interact with colleagues or other stakeholders.

- f. *SSD Point of Contact for the Social Media Access Policy.*
- g. *Appendix A: Acceptable Use Policy Acknowledgement* to be signed by each SSD staff member, agent and/or contractor receiving access.
- h. *Appendix B: List of Employees*  
SSDs must maintain a comprehensive listing of the names, HSEN User IDs (where applicable) and job title of those employees accessing social media sites.
- i. *Optional Provisions*

SSDs may choose to incorporate additional practices or policies regarding social media use that are consistent with the guidance provided herein and that are not contrary to any applicable state and federal laws, rules, and regulations, or any SSD policies.

#### **Issued By**

**Name: Krista Rock**  
**Title: General Counsel, OTDA**  
**Division/Office: Office of Legal Affairs**

**Name: Suzanne E. Miles-Gustave, Esq.**  
**Title: Deputy Commissioner and General Counsel, OCFS**  
**Division/Office: Office of Legal Affairs**