Local Commissioners Memorandum

Section 1

Transmittal:	15-LCM-16
To:	Social Services District Commissioners
Issuing Division/Office:	OTDA -AQI and CCWB and OLA
Date:	September 29, 2015
Subject:	Establishing a Social Media Access Policy for Social Services District Investigators
Contact Person(s):	Carmela Pellegrino at (518) 474-9502
Attachments:	
Attachment Available On – Line:	

Section 2

I. Purpose

This LCM provides local Social Services Districts (SSD) with information and guidance regarding the use of Social Media by SSD investigators. 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/social%20media). 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 for investigative purposes, SSDs must seek the guidance of the SSD's attorney and their Human Resources experts when drafting the SSD Social Media Access policy. SSDs are also reminded of their obligation to comply with the terms of service of all social media sites, 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 revises and supersedes 13-LCM-13 Social Media Access by Local District Child Support and Fraud Investigators, originally issued October 13, 2013. Also, please note the NYS Office of Information and Technology Services has issued NYS-G10-001, available at https://www.its.ny.gov/sites/default/files/documents/secure_use_of_social_media_guideline_0.pdf, NYS-P11-001, available at https://www.its.ny.gov/sites/default/files/documents/nys-p11-001.pdf, and 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 does not encompass all issues identified by OTDA for purposes of this LCM.

II. Background

SSD staff directly involved in activities such as Front End Detection System (FEDS), Field Investigations, Criminal Prosecutions and Child Support Investigations seek information from a variety of sources in the course of their investigations. Many investigators believe that the subjects of their investigations often reveal relevant, material information on social networking sites regarding their cases that may not be readily available elsewhere. In the past, SSD staff have requested access to these sites, such as Facebook, through the HSEN, but in SSDs not utilizing the HSEN, access was granted by other means controlled by the SSD or county. Given the significant risks presented in granting unrestricted access to social networking sites, some limited scope pilots had previously been approved in the past.

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

Each SSD allowing access to social media sites for investigations shall develop and implement a Social Media Access Policy which must provide investigators with a comprehensive overview in appropriate investigative techniques that must be followed when utilizing social media sites regardless of whether or not such access occurs via use of the HSEN. Each SSD shall make the Social Media Access Policy available to OTDA upon request. Each Social Media Access Policy must contain the required elements described below:

a. Objectives and Expected Outcomes

Each Social Media Access Policy must outline the objectives and expected outcomes regarding the use of social media during investigations. This section should emphasize that social media policies must be consistent with all applicable state and federal laws, rules, regulations, as well as SSD policies. Any other SSD investigative policies relevant to the use of social media should also be enumerated in this section (i.e. any policies relevant to acceptable use of the internet, limitations on the sites to be utilized and/or investigative techniques relevant to search engines). Furthermore, the policy must address the use of personal portable devices, such as personal cell phones, tablets, iPads, and/or laptops, along with the use of investigator's personal accounts. The use of personal portable devices and personal accounts is strongly discouraged based on security, compliance, and confidentiality concerns and considerations.

b. Scope

This section must articulate which job titles in the agency should have or will have access to social media for investigative purposes. 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, who administers access, and who monitors access. Multiple roles may not be held by one individual.

c. Authorization Levels

In this section, SSDs must outline the policy for gaining supervisory approval to access social media sites for investigative purposes. This section should include how and when social media sites should be accessed.

d. Intended Level of Engagement

SSDs must identify the intended level of engagement each investigator will take once granted access to social media sites. The level of engagement can be categorized as Apparent/Overt or Discrete.

- **Apparent/Overt** is when there is no interaction between the investigator and the subject of the investigation. The information reviewed by the investigator is open and available to the public in general. An example of an apparent level of engagement is an investigator searching the public Twitter or Facebook profile of the subject of an investigation. The information is gained without interaction between the investigator and the subject, and the information is available for general public use.

- **Discrete** is when the investigator's identity is not readily apparent to the subject of the investigation and there is no interaction between the subject and the investigator. An example of this would include utilizing tools to conceal the Internet Protocol (IP) address of the investigator to avoid tracking on various social mediums, including blogs.

If the SSD intends to utilize more than one level of engagement, the SSD must articulate the authorization necessary for each level of engagement.

The SSD must ensure that investigators authorized to utilize social media will adhere to the terms and conditions for each social media site in addition to adhering to all applicable State and Federal laws and regulations, including but not limited to the Fourth Amendment, which protects one's reasonable expectation of privacy through the prohibition of an unlawful search and seizure. Publically available information on social media sites may be utilized in investigations. However, investigators must not conduct any investigation utilizing a fake profile or alias unless specific authorization to do so has been obtained from the specific social media site in question. Such authorization must be in writing and retained by the SSD. This authorization must be made available to OTDA upon request.

e. Monitoring Plan

SSDs are asked to outline how the use of social media by investigators will be monitored by SSD management. In this section, SSDs must set out how often the applicable Social Media Access Plan will be reviewed and updated by the SSD. At a minimum, the SSD must perform an annual review and update of the plan, along with an annual review and update of the listing of those with access to social media, along with their scope of access.

f. Confidentiality Requirements

This section must set out the confidentiality requirements all SSD staff must follow when utilizing social media sites and the consequences in the event said requirements are not followed.

g. SSD Point of Contact for both the Social Media Access Policy and the listing of those with authorized access

h. Appendix A: Acceptable Use Policy Acknowledgement to be Signed by Each SSD staff member, agent and/or contractor Receiving Access

i. 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 for investigative purposes.

j. Optional Appendix C: List of Social Networking Sites To Be Utilized

k. Optional Provisions

SSDs may choose to incorporate additional practices or policies regarding social media use in investigations. Considerations include whether the investigator will be required to verify or authenticate the information taken from the social media site. This section can highlight the investigators role in the investigation in conjunction with the obligations set forth in the Fourth Amendment. In addition, the SSD may outline how, if at all, investigations utilizing social media will be documented (e.g. what information was collected, when the information was accessed, how the information was accessed, etc.). SSDs may also articulate what, if any, record retention requirements are imposed on the documentation.

Issued By
Name: Kevin Kehmna
Title: Director
Division/Office: Audit and Quality Improvement

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

Name: Eileen Stack
Title: Deputy Commissioner
Division/Office: Center for Child Well-Being