Policy 3-101.5 Social Media Non-Covert Investigation Policy

Effective Date: *July 31, 2015*
Applicability: *All regular, temporary and volunteer employees*
References: *ORPC 4.2 and 4.3*

---

1. Non-Covert Investigative Use

Social media can be a valuable source of information for use in Department of Justice (DOJ) work. Such information can be used to, among other things, identify witnesses, locate witnesses, locate a party, gather information about a party's employment or assets, obtain admissions for use in litigation, gather information about expert witnesses, and discover evidence of a violation of a law.

This policy governs the acquisition and use of **public** information from social media websites through passive means for any DOJ-related purpose.

This policy does not address the acquisition of **non-public** information from social media sites. Although it may be legally and ethically permissible to obtain non-public information, such activities should be approached with caution and may only be undertaken with the prior approval of a Division Administrator or designee.

Further, this policy does not address the use, covert or otherwise, of social media for purposes of criminal investigations by the Criminal Justice Division.

This policy also does not address the use of social media sites to disseminate agency-related information to the public.

2. Public vs. Non-Public Information; Passive vs. Active Use

Personal pages on social media sites can be opened for viewing by the public or can have access restrictions. This will depend on the privacy settings chosen by each individual social media site user. Information that can be viewed on a social media site by every other user of that site is considered publicly available. Viewing such information does not require interaction with a user and is considered passive conduct.

In contrast, information on social media sites that can only be viewed with the permission of a user is considered private, or non-public, information. Accessing non-public information is considered active conduct and implicates a number of ethical and legal considerations. Such use is not permitted under this policy.

3. Passive Viewing of Information on Social Media Sites

Passive viewing of information on social media sites is permissible for DOJ employees. Authorization requires prior written approval of a supervisor (See paragraph 5 below). This includes social media sites that require logging into the site as a user in order to view other users' information. This policy does not authorize interacting with social media site users for investigative purposes through the use of "tweets," "friending," or any other method except as described below in section 4.

4. Messaging

If it is not possible or practical to contact a site user in another way, it is permissible to send a message on a social media site asking the site user to contact an individual or office with DOJ with contact information. Every message sent to a site must clearly explain the reason the DOJ employee is trying to contact the user.

However, such contact raises potential ethical considerations. ORPC 4.2 prohibits a lawyer from contacting a social media site user who is represented by counsel. ORPC 4.3 provides that when contacting an unrepresented party a lawyer may not state or imply that the lawyer is disinterested. In addition, if a lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter, the lawyer shall make reasonable efforts to correct the misunderstanding. Lastly, ORPC 5.3 provides that a lawyer having direct supervisory authority over a non-lawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer. Consequently, these ethical concerns apply to non-lawyers contacting represented parties as well (e.g., Division of Child Support employees). Therefore, any message to a site user requesting contact information should include a statement making it clear that, if the site user is represented in the matter, the site user should request the site user/party's attorney to contact the DOJ.

5. Related Policy

This policy should be read in conjunction with DOJ Policy 3-101, which authorizes internet access if it is necessary to perform an assignment or if it is related to an activity that has been approved by DOJ. DOJ Policy 3-101(4)(i)(4) provides that work-related use of social media sites such as Myspace or Facebook requires prior written approval from a supervisor and the Administrative Services' Information Services Section (IS). Each Division shall establish a process for identifying the employees who will be authorized to access social media sites for DOJ work and enabling those employees to obtain written authorization using the DOJ *Authorization for Investigative Use of Social Media* form. See Appendix 3-101.5. **Social media site use authorized by this policy assumes an employee has obtained prior written approval.**

6. DOJ Computer Network Security

Accessing social media sites while logged onto the DOJ computer network may compromise network security. DOJ employees who are authorized to access social media sites must do so only from authorized DOJ devices (computers, laptops, smartphones, tablets, etc.) or through remote access into the DOJ network. Accessing DOJ-maintained social media sites accounts or accessing social media sites for DOJ purposes on personal devices without accessing the DOJ network is prohibited.

7. Personal Safety and Confidentiality

Social media sites should only be accessed using DOJ-created social media accounts. DOJ employees should not log into social media sites using personal accounts. Use of personal accounts could compromise an employee's safety because of the potential to reveal personal identifying information. In addition, much of the work of the department involves confidential and sensitive matters. Conducting investigative work using personal accounts creates a substantial risk that such information may be improperly disclosed.

8. Use of Information from a User's Social Media Site Provided by a Party or Third Party

It is permissible for attorneys and non-attorney staff to use information obtained independently by third parties from a social media site provided it was legally obtained. The value and admissibility of such information may be questionable if the method of acquisition cannot be verified. The best practice would be to require the party or third party to demonstrate, using a computer, how the information was obtained.