pennsylvania
OFFICE OF STATE
INSPECTOR GENERAL

POLICY

PERSONAL USE OF SOCIAL MEDIA

Date:	By Direction Of:
October 18, 2021	Lucas M. Miller, State Inspector General

A. Purpose & Scope.

The purpose of this policy is to define the Office of State Inspector General's (OSIG) policy and procedures on the personal use of social media by all OSIG employees. Social media (and related technology) should be broadly understood for purposes of this policy to include blogs, podcasts, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites such as Facebook, Instagram, Twitter, TikTok and YouTube, and other sites and services that permit users to share information with others in a contemporaneous manner. This policy also includes future social media technologies and applications that may not yet be contemplated. Failure to abide by this policy may result in disciplinary action, up to and including termination.

B. Policy.

OSIG recognizes the role that social media plays in the personal lives of some OSIG employees. However, the personal use of social media can have a negative impact on employees in their official capacity and on the agency. The OSIG has the right to maintain an orderly, safe and efficient work environment consistent with its organizational values and mission. To this end, the OSIG trusts and expects employees to exercise personal responsibility whenever they participate in social media activities. OSIG employees are free to post their personal views on social media platforms to the extent that such views are not violative of OSIG or Commonwealth policies and procedures. Moreover, use of these sites may violate the rights of others when untrue, defamatory or legally protected information is posted without permission.

Employees must also keep in mind that once information appears online, it can become part of a permanent record, even if the author later "deletes" it. Everything written on the Web can be traced back to its author, often very easily.

Employees must abide by the terms and conditions set forth by social media websites.

OSIG employees should not use social media in a way which may tarnish the image or mission of the OSIG and/or bring the credibility of the employee into disrepute. Any evidence of a violation of state and federal law will be referred to the proper authorities.

OSIG employees should be cognizant of the fact that their social media activities may have a negative impact on their image and the image of the OSIG.

Employees should use their best judgment to ensure that materials being posted are neither inappropriate not harmful to the OSIG or its employees.

C. Procedures.

OSIG employees shall abide by the following when using social media.

1. OSIG employees may not use social media in a manner that interferes with their job duties, impairs working relationships of the agency, breaches confidentiality, or negatively impacts the public perception of the agency.

2. OSIG employees are cautioned that speech on or off duty, made pursuant to their official duties – i.e., that owes its existence to the employee's professional duties and responsibilities – is not protected speech under the First Amendment and may form the basis for discipline if deemed detrimental to the agency. Employees must assume that their speech and related activity on social media sites will reflect upon this agency.

3. OSIG employees are prohibited from posting, transmitting, or otherwise disseminating any information to which they have access as a result of their employment without prior written permission from the State Inspector General or his/her designee. OSIG employees will not make any statements, speeches, appearances, and endorsements or publish materials that could reasonably be considered to represent the views or positions of this agency without express authorization from the State Inspector General or his/her designee.

4. For safety and security reasons, OSIG employees are cautioned not to disclose their employment, nor that of their co-workers, with OSIG nor shall they post information pertaining to any other employee of the agency without their express written permission. As such, employees are directed not to do the following:

    - Display agency logos, patches, badges, insignias, uniforms, equipment, vehicles, letterhead or similar identifying items on any web pages, or

    - Employees who may reasonably be expected to work in undercover operations, should not post any form of visual or personal identification.

5. When using social media, OSIG employees should be mindful that their speech becomes part of the worldwide electronic domain. Therefore, adherence to the OSIG code of conduct policy is required in the personal use of social media. Although not an exhaustive list, some specific examples of prohibited social media conduct include posting:

    - Speech containing sexually explicit language or, images.
    - Speech that expresses bias against any individual or group on any basis including race, gender or gender identity, ethnicity religion, age, disability or any protected class of individuals.
    - Speech involving themselves or other OSIG employees reflecting behavior that would reasonably be considered reckless or irresponsible.
    - Speech that is harassing or creates a hostile work environment.
    - Speech that is defamatory or libelous.

6. Engaging in prohibited speech noted herein, may provide grounds for undermining or impeaching an employee's credibility or testimony in criminal proceedings. If employees encounter an antagonistic situation while on social media, the employee should disengage from the dialogue in a polite manner.

7. OSIG employees may be subject to civil litigation for:

    - Publishing or posting false information that harms the reputation of another person, group, or organization (defamation);
    - Publishing or posting private facts and personal information about someone without their permission that has not been previously revealed to the public, is not of legitimate public concern, and would be offensive to a reasonable person;
    - Using someone else's name, likeness, or other personal attributes without that person's permission for any purpose, exploitative or otherwise; or
    - Publishing the creative work of another, trademarks, copyrighted material, or certain confidential business information without the permission of the owner.

8. Be aware that privacy settings and social media sites are constantly in flux. Never assume that personal information posted on such sites is protected.

9. Expect that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the agency at any time without prior notice.

10. Reporting violations. Any employee becoming aware of or having personal knowledge of a posting or of any website or web page in violation of the provision of this policy are required to notify his or her supervisor immediately for follow-up action.

D. Additional Information.

For additional information relating to this policy, contact your immediate supervisor.