NEW YORK STATE Department of Corrections and Community Supervision **DIRECTIVE**	TITLE **Social Media Policy for Department Employees**		NO. 2825 DATE 09/27/22
SUPERSEDES DIR #9803 Dtd. 12/09/20	DISTRIBUTION A B	PAGES PAGE 1 OF 6	DATE LAST REVISED
REFERENCES (Include but are not limited to) Public Officers Law §74(3)(h); Directives #2810, #2824; ITS Policy No. NYS-P14-001	APPROVING AUTHORITY		

I. PURPOSE: To provide clear and concise direction to Department staff involved in the use of social media for personal and professional purposes. To establish guidelines for cyber-vetting for work-related activities and community-based resources.

II. POLICY: The Department of Corrections and Community Supervision (DOCCS) will permit the use of social media by the Office of Public Information, as a recruitment tool and as an investigative tool when seeking evidence or information about matters relevant to its mission.

Social media content shall adhere to applicable laws, regulations, and Departmental directives, including all information technology and records management directives.

NOTE: For information related to the personal use of social media by staff, refer to DOCCS Directive #2824, "Use of Electronic Mail (E-Mail)."

III. DEFINITIONS

A. Social Media: Forms of electronic communication (e.g., websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (e.g., videos).

B. Cyber-Vetting: The use of social media to investigate and evaluate an individual or an entity's online presence or internet reputation (netrep) on social networking services such as, but not limited to, Facebook, Instagram, TikTok, Bebo, Twitter, and LinkedIn.

C. Associates: Individuals that identified individuals interact with including, but not limited to, family, friends, partners, companions, counselors, community service providers, etc.

D. Apparent/Overt Use: A review of public pages. Information is publicly available to anyone.

E. Discreet Use: Officer/Department identity is not apparent. When approved, an officer may use a pseudonym and anonymized IP address.

F. Covert Use: Officer/Department actively creates a fictitious identity to directly interact with others. Essentially "undercover" work that requires specific training.

G. Internet Protocol Address (IP Address): A numerical label assigned to each computer device used to identify itself and communicate with other devices in the IP network.

H. Internet Service Provider (ISP): A company that provides subscribers with access to the internet.

I. Screen Name: The name a user chooses to use when communicating with others online.

IV. GUIDELINES FOR PROFESSIONAL USE OF SOCIAL MEDIA

A. Community Supervision: The monitoring of social media can be an effective supervision tool used to gather intelligence and/or monitor a parolee's activities and whereabouts in the community. Periodic cyber-vetting is particularly recommended for specialized caseloads such as Sex Offender, Strict and Intensive Supervision and Treatment (SIST), Gang, and UBER. The same standards, principles, and guidelines that apply to DOCCS employees in the performance of their assigned duties apply to social media use.

Staff are encouraged to utilize the internet for the purpose of identifying and evaluating community-based resources and treatment providers that may be utilized by the parolee population.

1. Acceptable forms of social media monitoring include:

   a. Apparent/Overt Use

      (1) Involves accessing social networking sites without any interaction with the targeted parolee.

      (2) Requires no special training or authorization.

      EXAMPLE: Conducting a Google search of a parolee's name.

   b. Discreet Use

      (1) Involves concealing the identity of the employee, but there is no online interaction with the targeted parolee.

      (2) Requires the creation of an assumed name (pseudonym) as a screen name and a discreet email address to be approved by a Bureau Chief and registered on DOCCS Form #CS9803A, "Registration of Staff Social Media Account."

      EXAMPLE: Viewing a parolee's Facebook page or Twitter account by utilizing an account created with a Department-registered pseudonym.

   c. Covert Use: Involves concealing the identity of the employee and requires online interaction with the targeted parolee to gain information.

      Requires the following:

      (1) Creation of an assumed name (pseudonym) as a screen name and a discreet email address to be approved by a Bureau Chief and registered on Form #CS9803A.

      (2) Special training.

      (3) Specific authorization for engaging in interaction with each targeted parolee must be obtained from the respective Bureau Chief prior to any online interaction between staff and the targeted parolee.

      EXAMPLE: Posting a message or making a "friend request" on a parolee's social media page by utilizing an account created with a Department-registered pseudonym.

NOTE: A user's IP Address is registered each time a website is visited. Caution should be exercised when visiting a website suspected to be owned or operated by parolees or their associates, as anonymity may be compromised through a user's IP Address.

2. Community Supervision staff utilizing social media as an investigative tool will:
   a. Use only DOCCS-authorized electronic devices throughout the investigation.
   b. Register the screen name and email with DOCCS on Form #CS9803A.
   c. Obtain authorization for covert use from the Bureau Chief prior to engaging in interaction with targeted parolee.
   d. Immediately alert supervisory staff of the discovery of new criminal activity, a violation of release, or behavior that may compromise public safety, the safety of DOCCS employees, or the safety of a parolee. Supervisory staff will evaluate findings and take appropriate action.
   e. Record all of the findings of the investigation:
      (1) Narratives are to be made as a confidential entry in the Case Management System (CMS) F-9 screen.
      (2) Email/ISP/Screen names of parolees are to be entered in the CMS F-24 screen.
      (3) Printed copies of a parolee's social media page that may constitute evidence of a possible crime or violation of release are to be filed in the case folder.
3. Community Supervision staff utilizing social media as an investigative tool will <u>not</u>:
   a. Use their personal cell phone or other personal telecommunications device to contact or communicate with parolees.
   b. Use their personal social media account or personal account information to access the parolee's social media content.
   c. Use another individual's personal account without their consent and the approval of the Bureau Chief.
   d. Post content that jeopardizes the confidentiality or safety of an employee, or parolee, their associates, or victims.
   e. Establish a false identity of a real-life person in order to gain the trust or elicit a response from a parolee or their associates.

B. <u>Office of Public Information</u>: DOCCS has an established Facebook account that is operated and maintained by the Public Information Office (PIO). PIO is responsible for monitoring the postings and content contained therein.

Community Supervision Area Offices are not authorized to establish social media web pages that represent the activities of their specific area office or region. Area Office staff seeking to post content to the Department's Facebook account must have the approval of the Bureau Chief, and submissions must be forwarded to the PIO for posting via the chain of command.

C. Office of Special Investigations (OSI): Social media is a valuable investigative tool when seeking evidence or information about matters relevant to OSI's mission, such as: locating wanted persons, terrorist recruitment, photos or videos of a criminal activity by a participant or observer, crimes perpetrated online (e.g., cyber-stalking), and evidence of misconduct by DOCCS employees. This is a non-inclusive list for illustrative purposes. OSI Investigators shall follow the applicable laws, directives, and OSI policies when utilizing social media during an investigation.

V. GUIDELINES FOR PERSONAL USE OF SOCIAL MEDIA:

A. For the purpose of this Directive, social media means any form of electronic communication (e.g., websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (e.g., videos).

DOCCS recognizes the role that social media plays in the personal lives of our employees and respects our employees' rights to free expression as private individuals.

Employees are advised that personal use of social media can reflect on them in their official capacity, as well as on DOCCS and other State governmental entities. Employees are reminded that DOCCS is subject to close scrutiny by the public and the media. An employee's personal use of social media can reflect on the credibility of DOCCS as a Department. Social media posts made by employees can be used in litigation against the Department and the employee, and employees should assume that posts made on social media will be found, scrutinized, and become subjects for discussion in judicial proceedings. This directive provides prohibitions and cautionary information on the use of personal social media by DOCCS employees.

Staff should be sensitive to the fact that information posted on social media sites clearly reflects on the individual and may also reflect on the individual's professional life. Consequently, staff should use discretion when posting information on these sites and be conscious of the potential perceptions of and responses to the information. It is important to remember that once information is posted on a social media site, it can be captured and used in ways not originally intended. It is nearly impossible to restrict, as it often lives on in copies, archives, back-ups, and memory cache.

B. DOCCS employees shall abide by the following when using personal social media:

1. Employees are free to express themselves as private citizens on social media to the extent that their speech does not impair working relationships, impede the performance of duties, impair discipline and harmony among co-workers, compromise the safety or security of any DOCCS facility, or reflect discredit on DOCCS or its personnel.
2. Employees are prohibited from posting on social media anything meant to intentionally harm someone's reputation or that can contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by DOCCS' policies or directives, or by law.
3. As state employees, DOCCS employees are cautioned that speech, whether on or off duty, made pursuant to their official duties is not protected speech under the First Amendment and may form the basis for discipline if deemed detrimental to DOCCS.

4. Employees are further cautioned that as state employees, certain types of private speech may not be protected under the First Amendment and may form the basis of discipline if sufficiently detrimental to DOCCS and its interests.
5. Employees shall not post, transmit, or otherwise disseminate any information which they have access to as the result of their employment without express written permission from DOCCS.
6. Employees shall not make any personal statements, endorsements, representations, or publish any materials that could reasonably be considered to represent the views or positions of DOCCS without express written permission. This shall include but not limited to the use of hashtags, sharing links to the Department website, or otherwise tagging the Department in a post.
    a. If a personal email, posting, or other electronic message could be construed to be an official communication, a disclaimer is strongly recommended. For example, “The views and opinions expressed are solely those of the author and do not necessarily reflect those of the Department of Corrections and Community Supervision or the State of New York.”
7. For safety and security reasons, employees are cautioned not to disclose their employment with DOCCS on public social media pages or websites. As such, DOCCS employees are encouraged to not display DOCCS badges, logos, uniforms, or similar identifying items on such sites.
8. Employees should conduct themselves in a manner consistent with the highest level of integrity, decorum, and professionalism in their personal use of social media. DOCCS employees are subject to Section 2.1, Personal Conduct, of the Employees Manual, which provides “No employee, whether on or off duty, shall so comport himself or herself as to reflect discredit upon the Department or its personnel.” As State employees, DOCCS employees are also subject to Public Officers Law §74(3)(h) which provides “An officer or employee of a state agency, member of the legislature or legislative employee should endeavor to pursue a course of conduct which will not raise suspicion among the public that he or she is likely to be engaged in acts that are in violation of his or her trust.” DOCCS employees should refrain from the following in their public social media use:
    a. Distributing, transmitting, posting, or storing any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, sexually exploitative, sexually explicit, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate.
    b. Distributing, transmitting, posting, or storing electronic communications, photos, video, or audio involving themselves or other DOCCS employees reflecting behavior that would reasonably be considered reckless, irresponsible, or unprofessional.
9. Employees shall respect the privacy of DOCCS staff, incarcerated individuals, and releasees and shall not post any identifying information, including but not limited to names, addresses, photos, videos, email addresses, and phone numbers, about any of these individuals without permission.

10. Employees choosing to use personal social media are encouraged to understand and utilize the privacy settings on social media sites and should never assume that personal information posted on such sites is fully private or otherwise protected from exposure. Employees should assume that posts that are intended to be private may become public.
11. Employees should expect that any information created, transmitted, downloaded, exchanged, or discussed in a public forum may be accessed by DOCCS at any time without prior notice.
12. Employees who are required or permitted to use social media as part of their official job duties shall conduct themselves consistent with this policy and any other DOCCS social media policy, and, where applicable, the direction of their supervisors.
13. Employees are personally responsible for the content personally published on blogs, social media, or any other user-generated media.
14. Always remember that anything published on social media can go viral, no matter what your privacy settings may be.
15. Employees should assume that posts or accounts that have been deleted or disabled can be accessed. The internet never forgets.