NEW YORK STATE Corrections and Community Supervision **DIRECTIVE**	TITLE **Social Media Policy for Community Supervision Staff**		NO. 9803 DATE 05/02/2019
SUPERSEDES	DISTRIBUTION A	PAGES PAGE 1 OF 3	DATE LAST REVISED
REFERENCES (Include but are not limited to) Directives #2810, #2824; ITS Policy No. NYS-P14-001	APPROVING AUTHORITY		

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

II. POLICY: The Department of Corrections and Community Supervision (DOCCS) will permit the use of social media as an investigative tool when seeking evidence or information about matters relevant to its mission, such as potential parole violative behaviors, wanted persons, gang participation and retaliations, photos or videos of a crime posted by parolees, and crimes perpetrated online (e.g., cyber stalking).

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

1. 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).
2. 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 Facebook, Myspace, Twitter, Bebo, and LinkedIn.
3. Associates: Individuals that parolees interact with including, but not limited to, family, friends, partners, companions, counselors, community service providers, etc.
4. Apparent/Overt Use: An officer reviews parolee's public pages. Information is publicly available to anyone.
5. Discreet Use: Officer/Department identity is not apparent. When approved, an officer may use a pseudonym and anonymized IP address.
6. Covert Use: Officer/Department actively creates a fictitious identity to directly interact with parolees. Essentially "undercover" work that requires specific training.
7. 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.
8. Internet Service Provider (ISP): A company that provides subscribers with access to the internet.
9. Screen Name: The name a user chooses to use when communicating with others online.

IV. PROCEDURE

A. Guidelines for Professional Use of Social Media: 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; and

      (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; and
   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; and
      (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 not:
   a. Use their personal social media account or personal account information to access the social media content;
   b. Use another individual's personal account without his or her consent and the approval of the Bureau Chief;
   c. Post content that jeopardizes the confidentiality or safety of an employee, or parolee, his or her associates, or victims; and
   d. Establish a false identity of a real-life person in order to gain the trust or elicit a response from a parolee or his or her associates.

B. Guidelines for Departmental Use of Social Media: The New York State Department of Corrections and Community Supervision 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 bureau 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 PIO for posting via the chain of command.

REGISTRATION OF STAFF SOCIAL MEDIA ACCOUNT

Name: _____ Title: _____

Bureau/Office Assignment: _____

REGISTRATION OF SOCIAL MEDIA ACCOUNT

☐ Social Media Outlet (i.e. Facebook, Instagram, Twitter, etc.): _____

☐ User/Screen Name: _____

☐ Email Address Used to establish account: _____

NOTE: The screen name and email address listed above is solely for professional use, for the purpose of furthering the mission of the New York State Department of Corrections and Community Supervision. It is never to be used for personal activity on social media. You must provide the Department with any passwords associated with this account upon the direction of your Bureau Chief.

Parole Officer: Signature: _____

Reviewed by:

Sr. Parole Officer: Name: _____ Signature: _____ Date: _____

Approved by:
Bureau Chief: Name: _____ Signature: _____ Date: _____

UNREGISTRATION OF SOCIAL MEDIA ACCOUNT

☐ Social Media Outlet (i.e. Facebook, Instagram, Twitter, etc.): _____

☐ User/Screen Name: _____

☐ Email Address Used: _____

REASON: _____

NOTE: Once the above screen name and email address is unregistered, it cannot be used for any other social media-related activity without re-registration and approval by the Bureau Chief.

Parole Officer: Signature: _____

Reviewed by:

Sr. Parole Officer: Name: _____ Signature: _____ Date: _____

Approved by:
Bureau Chief: Name: _____ Signature: _____ Date:_____

***Scan and E-Mail form to*:** DOCCS.SM.SOCIALMEDIAFORM.CSOC

CC: Regional Director/Assistant Regional Director, OSI, PIO

Form #CS9803A (05/19)