	Administrative General Order | 8.08 Use of Social Media	PAGE 1 OF 5
	SUBJECT **Virginia Beach Police Department Written Directive** Chapter 8 – Criminal Investigations	EFFECTIVE DATE **09/07/2017** ORIGINATOR/REVIEW Investigative Division
	DISTRIBUTION ALL	**CALEA:**
BY THE AUTHORITY OF THE CHIEF OF POLICE:		

Purpose:

The purpose of this policy is to clarify the department's understanding, access, use, and retention of information garnished from social media sites.

Policy:

Data contained within social networking sites may assist law enforcement in gathering timely information in the furtherance of crime prevention, preservation of public order, and the investigation of criminal activity. Use of social media resources shall be consistent with all applicable laws and City and Departmental policies.

Definitions:

Crime Analysis and Situational Assessment Reports – Analytic activities and documents that enable department personnel to identify and understand trends, causes, relationships, and potential indicia of criminal activity.

Criminal Intelligence Information—Data which meets criminal intelligence collection criteria outlined in 28 CFR Part 23 and which has been evaluated and determined to be relevant to the identification of criminal activity engaged in by individuals, or organizations, which are reasonably suspected of involvement in criminal activity.

Public Domain- Any internet resource that is open and available to anyone.

Online Alias— An online identity encompassing identifiers, such as name and date of birth, differing from the employee's actual identifiers.

Online Undercover Activity— The utilization of an online alias to engage in interactions with a person via social media sites that may or may not be in the public domain.

Social Media Websites—Sites which focus on building online communities of people who share interests and activities and/or exploring the interests and activities of others. Social media websites are further categorized by Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), micro blogging sites (Twitter, Nixle), photo-and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit). The absence of an explicit reference to a specific social media website does not limit the application of this policy.

Social Media Monitoring Tool—A resource used to capture data and monitor social media sites by utilizing automated tools such as web crawlers and word search functions to analyze data, develop trends,

or collect information. [redacted]

Page- The specific portion of a social media website where content is displayed and managed by an individual or individuals.

Post- Content an individual shares on a social media site or the act of publishing content to a site.

Valid Law Enforcement Purpose—A purpose for information/intelligence gathering development, or collection, use, retention, or sharing that furthers the authorized functions and activities of a law enforcement agency, which may include the prevention of crime, ensuring the safety of the public, and furthering officer safety, while adhering to law and agency policy designed to protect the privacy, civil rights, and civil liberties of Americans.

Utilization of Social Media

When a member of the department requires the use of social networking websites to conduct investigations or research, the following procedure will be used:

Social media may be used by personnel for a valid law enforcement purpose. The following are valid law enforcement purposes:

- Crime analysis and situational assessment reports;
- Criminal intelligence development; and
- Criminal investigations

While on duty, employees will utilize social media, access social media websites, online aliases, and social media monitoring tools for a valid law enforcement purpose. The utilization of an online alias or social media monitoring tool for personal use is prohibited and is considered employee misconduct.

Employees will only utilize social media to seek or retain information that:

1. Is based upon a criminal predicate or threat to public safety; or
2. Is based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed an identifiable criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal conduct or activity (28 CFR Part 23 compliant and maintained by CIU); or
3. Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
4. Is useful in crime analysis or situational assessment reports for the administration of criminal justice and public safety.

The department will not utilize social media to seek or retain information about:

1. Individuals or organizations solely on the basis of their religious, political, social views or activities; or
2. An individual's participation in a particular non-criminal organization or lawful event; or
3. An individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation unless such information is relevant to the individual's criminal conduct or

activity or if required to identify the individual; or

4. An individual's age other than to determine if someone is a minor unless such information is relevant to the individual's criminal conduct or activity or if required to identify the individual.

The Virginia Beach Police Department will not directly or indirectly receive, seek, accept, or retain information from:

1. An individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if there is reason to believe that the information provider is legally prohibited from obtaining or disclosing the information; or
2. A source that used prohibited means to gather the information.

Authorization to Access Social Media Websites

This section addresses the authorization necessary to utilize social media and access social media websites for crime analysis and situational awareness/assessment reports; intelligence development; and criminal investigations.

1. Public Domain- No authorization is necessary for general research, topical information or other law enforcement uses that do not require the acquisition of an online alias.

2. Online Alias- An online alias may only be used to seek or retain information that:
   - Is based upon a criminal predicate or threat to public safety; or is based upon reasonable suspicion that an identifiable individual, regardless of citizenship or U.S. residency status, or organization has committed a criminal offense or is involved in or is planning criminal conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal conduct or activity (in compliance with 28 CFR Part 28 and maintained by CIU); or
   - Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
   - Is useful in crime analysis or situational assessment reports for the administration of criminal justice and public safety.

3. Authorization for Online Aliases
   - Prior to generating an online alias, personnel shall submit a request for an online alias (Utilize PD-26 form) to their commanding officer.
   - The request must contain the following information:
     - Purpose for the request (i.e. type of investigative activity);
     - Username
     - Copy of each URL (specific to every social media site utilizing the approval-pending alias)
     - Identifiers to be utilized for the online alias, such as email address, username and date of birth. Do not include password(s) for online aliases and ensure password(s) are secured at all times; and
     - Photograph(s) to be used with online alias to ensure anonymity

   - The Commanding Officer must evaluate the request to determine whether an online alias would serve a valid law enforcement purpose. The Commanding Officer or their designee

must maintain the requests for online alias and their status (approved/denied)

- The use of an approved alias shall only be utilized for the purpose of viewing social media information. With the exception of sending and accepting a friend request, no other communication or contact is authorized.

4. Authorization for Online Undercover Activity
   - Only department personnel actively assigned to Special Investigations are authorized to act in an online undercover capacity. This includes (but is not limited to) any form of electronic communication involving images, messages, emails, instant messages, videos, posts, or tweets.
   - Access and use of an online undercover account shall only be done utilizing an undercover IP address.

Authorization to Utilize Social Media Monitoring Tools

Department members actively assigned to the Criminal Intelligence Unit, Warrant Squad, or serving in a sworn crime analyst assignment are authorized to utilize social media monitoring tools purchased by the department. Access to and use of these accounts is strictly limited to the identification and investigation of criminal activity. Use of department purchased social media monitoring tools by anyone outside of the assigned account is prohibited. Account information will be maintained by the Criminal Intelligence supervisor.

Network Consideration

Officers utilizing a city network computer to access social media shall consider the risk that the department can be linked to the user of the social media account. City networks are established to prevent intrusion but allow limited access to officers to maintain the integrity of the network. Officers shall take careful consideration when utilizing a network not associated with the city or a city network.

All officers are encouraged to take the following steps to avoid identification of the department or user which could potentially harm an ongoing investigation or officer.

- When selecting your username or password ensure that it cannot be traced to the officer or department.
- Do not allow access or associate family, friends and coworkers to an alias account. Avoid using your alias account to access their pages to ensure they are not connected to your account.
- Use caution when clicking tweets, links, posts or advertisements while utilizing social media. Retweeting or liking a post can alert the user that you have monitored their page.
- Never open an attachment to an email from a sender that is not known to you or any other officer on the department.
- Delete all “spam” emails without actually opening the email.

Officers are encouraged to avoid using their home and/or any personal network to access social media when possible to ensure your personal information is not linked to the account. When conducting department business with a social media account it is incumbent upon the officer to take

necessary precautions to avoid personal information being transmitted or disseminated on the internet.

Source Reliability and Content Validity

Information developed from social media sites should be corroborated using traditional investigative tools including interviews, verification of address, verification of internet protocol address information, or other lawful means.
Information deemed necessary for court must be obtained through the appropriate search warrant or subpoena.

Off Duty Conduct

An employee who becomes aware of potential criminal activity via the Internet while off duty shall contact their supervisor if the activity involves a minor child or exigent circumstances. The supervisor shall determine the best course of action.

As soon as practical following awareness of the potential criminal activity the employee should provide a memorandum detailing a complete description of the information observed and specifics as to the action taken. The memorandum should be addressed to the appropriate detective/ supervisor via the officer's chain of command.

Dissemination

Any information that is gathered for the purpose of criminal intelligence shall immediately be forwarded to the SI Criminal Intelligence Unit which shall be responsible for all data storage and retention in accordance with current SI policies. Retention and dissemination of social media information will be the same as the type of file, whether a paper or electronic file, in which the information is located. For example, retention and dissemination of social media information within an intelligence file will be treated in the same manner as an intelligence file. Information developed during the course of a criminal investigation will be located in the investigative case file and retained and disseminated in the same manner as the investigative case file.