HUNTERSVILLE POLICE DEPARTMENT

Directive 1.39 Social Media

Effective Date: February 23, 2016	**Rescinds: General Order 1.39 Social Media, 8-12-13**
Revision Date: February 2017	**Approved: Cleveland L. Spruill Chief of Police**

CONTENTS

A. POLICY/PURPOSE

1. Social media provides a new and potentially valuable means of assisting the department and its personnel in meeting community outreach, problem-solving, investigative, crime prevention, and related objectives. This policy identifies potential uses that may be explored or expanded upon as deemed reasonable by administrative and supervisory personnel. The department also recognizes the role that these tools play in the personal lives of some department personnel. The personal use of social media can have bearing on departmental personnel in their official capacity. As such, this policy provides information of a precautionary nature as well as prohibitions on the use of social media by department personnel.

2. The Huntersville Police Department has a duty to protect the reputation of the organization and its employees, as well as guard against liability and potential legal risks. Since the functions of the Huntersville Police Department have a major impact upon the community, standards of conduct for HPD personnel are higher than standards applied to the general public. Employees will conduct themselves in a manner which does not bring discredit upon themselves, the HPD, the Town of Huntersville, or the community when utilizing social networking sites on and off duty.

3. It shall be the policy of the HPD to acknowledge that employees have a right to have personal web pages or sites and to allow employees to exercise that right to the extent possible without causing a decline in public confidence and respect for the HPD or the employee as a member of the HPD.

4. The Huntersville Police Department endorses the secure use of social media to enhance communication, collaboration, and information exchange; streamline processes; and foster productivity. This policy establishes this department's position on the utility and management of social media and provides guidance on its management, administration, and oversight. This policy is not meant to address one particular form of social media, rather social media in general, as advances in technology will occur and new tools will emerge.

B. DEFINITIONS

1. Blog*:* A self-published diary or commentary on a particular topic that may allow visitors to post responses, reactions, or comments. The term is short for "Web log."

2. Page: The specific portion of a social media website where content is displayed, and managed by an individual or individuals with administrator rights.

3. Crime Analysis and Situational Assessment Reports – Analytic activities to enable SBI to identify and understand trends, causes, and potential indicia of criminal activity, including terrorism.

4. Criminal Intelligence Information – Data which meets criminal intelligence collection criteria and which has been evaluated and determined to be relevant to the identification of criminal activity engaged in by individuals who or organizations which are reasonably suspected of involvement in criminal activity.

5. Criminal Nexus – Established when behavior or circumstances are related to an individual or organization's involvement or planned involvement in criminal activity or enterprise.

6. Online Alias – An online identity encompassing identifiers, such as name and date of birth, differing from the employee's actual identifiers, that uses a nongovernmental Internet Protocol address. Online alias may be used to monitor activity on social media websites or to engage in authorized online undercover activity.

7. 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 (i.e. "friending a person on Facebook").

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

9. Profile: Information that a user provides about himself or herself on a social networking site.

10. Public Domain –Any Internet resource that is open and available to anyone.

11. Social Media: A category of Internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), microblogging sites (Twitter, Nixle), photo- and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).

12. Social Media Monitoring Tool – A tool used to capture data and monitor social media sites by utilizing automated tools such as web crawlers and word search functions to make predictive analysis, develop trends, or collect information. Examples include Netbase, Twitterfall, Trackur, Tweetdeck, Socialmention, Socialpointer, and Plancast.

13. 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.

14. Social Networks: Online platforms where users can create profiles, share information, and socialize with others using a range of technologies.

15. Speech: Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

16. Web 2.0: The second generation of the World Wide Web focused on shareable, user-generated content, rather than static web pages. Some use this term interchangeably with social media.

17. Wiki: Web page(s) that can be edited collaboratively.

18. 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, furthering officer safety, and homeland and national security, while adhering to law and agency policy designed to protect the privacy, civil rights, and civil liberties of Americans.

C. DEPARTMENT SANCTIONED PRESENCE ON SOCIAL MEDIA NETWORKS

1. Where possible, each social media page shall include an introductory statement that clearly specifies the purpose and scope of the agency's presence on the website.

2. Where possible, the page(s) should link to the Department's official website.

3. Social media page(s) shall be designed for the target audience(s) such as youth or potential police recruits.

4. All Department social media sites or pages shall be approved by the Chief of Police or his or her designee and shall be administered by the Administrative Services Bureau Commander or as otherwise determined.

5. Where possible, social media pages shall clearly indicate they are maintained by the Department and shall have department contact information prominently displayed.

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

   (a) Content is subject to public records laws. Relevant records retention schedules apply to social media content.

   (b) Content must be managed, stored, and retrieved to comply with open records laws and e-discovery laws and policies.

7. Where possible, social media pages should state that the opinions expressed by visitors to the page(s) do not reflect the opinions of the Department.

   (a) Pages shall clearly indicate that posted comments will be monitored and that the department reserves the right to remove obscenities, off-topic comments, and personal attacks.

   (b) Pages shall clearly indicate that any content posted or submitted for posting is subject to public disclosure.

D. DEPARTMENT APPROVED USE OF SOCIAL MEDIA

1. Department personnel representing the Department via social media outlets shall do the following:

(a) Conduct themselves at all times as representatives of the department and, accordingly, shall adhere to all department standards of conduct and observe conventionally accepted protocols and proper decorum.

(b) Identify themselves as a member of the Department.

(c) Not make statements about the guilt or innocence of any suspect or arrestee, or comments concerning pending prosecutions, nor post, transmit, or otherwise disseminate confidential information, including photographs or videos, related to department training, activities, or work-related assignments without express written permission.

(d) Not conduct political activities or private business.

(e) The use of department computers by department personnel to access social media is prohibited without authorization.

(f) Department personnel use of personally owned devices to manage the department's social media activities or in the course of official duties is prohibited without express written permission.

(g) Employees shall observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.

E. POTENTIAL USES OF SOCIAL MEDIA

1. Social media is a valuable investigative tool when seeking evidence or information about:

   (a) Missing persons;
   (b) Wanted persons;
   (c) Gang participation;
   (d) Crimes perpetrated online (i.e., cyberbullying, cyberstalking); and
   (e) Photos or videos of a crime posted by a participant or observer.

2. Social media can be used for community outreach and engagement by:

   (a) providing crime prevention tips;
   (b) offering online-reporting opportunities;
   (c) sharing crime maps and data; and
   (d) soliciting tips about unsolved crimes (i.e., Crimestoppers, text-a-tip).

3. Social media can be used to make time-sensitive notifications related to:

   (a) Road closures;
   (b) Special events:
   (c) Weather emergencies; and
   (d) Missing or endangered persons.

4. Persons seeking employment and volunteer positions use the Internet to search for opportunities, and social media can be a valuable recruitment mechanism.

5. This Department has an obligation to include Internet-based content when conducting background investigations of job candidates.

(a) Searches should be conducted by a non-decision maker. Information pertaining to protected classes shall be filtered out prior to sharing any information found online with decision makers.

(b) Persons authorized to search Internet-based content should be deemed as holding a sensitive position.

(c) Search methods shall not involve techniques that are a violation of existing law.

(d) Vetting techniques shall be applied uniformly to all candidates.

(e) Every effort must be made to validate Internet-based information considered during the hiring process.

F. INVESTIGATIVE USE OF SOCIAL MEDIA

1. Social media may be a valuable investigative tool to detect and prevent criminal activity. Social media has been used for community outreach events such as providing crime prevention tips, providing crime maps, and soliciting tips about unsolved crimes. Social media may also be used to make time sensitive notifications regarding special events, weather emergencies, or missing or endangered persons. While social media is a new resource for law enforcement, employees must adhere to this policy to protect individuals' privacy, civil rights, and civil liberties and to prevent employee misconduct.

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

    (a) Pre-employment background investigations;

    (b) Crime analysis and situational assessment reports;

    (c) Criminal intelligence development; and

    (d) Criminal investigations.

3. While on duty, employees will utilize social media, access social media websites, online aliases, and social media monitoring tools only 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.

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

    (a) Is based upon a criminal predicate or threat to public safety; or

    (b) 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 (criminal intelligence information); or

(c) 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

(d) Is useful in crime analysis or situational assessment reports for the administration of criminal justice and public safety; or

(e) Is relevant to pre-employment background investigations.

5. The Department will not utilize social media to seek or retain information about:

(a) Individuals or organizations solely on the basis of their religious, political, social views or activities; or

(b) An individual's participation in a particular non-criminal organization or lawful event; or

(c) 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

(d) An individual's age other than to determine if someone is a minor.

6. The Department will not directly or indirectly receive, seek, accept, or retain information from:

(a) 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

(b) A source that used prohibited means to gather the information.

7. Authorization to Access Social Media Websites

(a) 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:

a. Is based upon a criminal predicate or threat to public safety; or

b. 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; or

c. 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

d. Is useful in crime analysis or situational assessment reports for the administration of criminal justice and public safety.

8. Authorization for Online Aliases for Investigative Purposes

(a) Sworn officers or criminal intelligence analysts must submit a request for an online alias. No other Department personnel are authorized to submit requests for an online alias or to use an online alias in the performance of their official duties.

(b) The request must contain the following information:

1) Purpose for the request (i.e. type of investigative activity);

2) Username;

3) Identifiers and pedigree 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

4) Photograph to be used with online alias, if applicable.

(c) The CRD Commander must evaluate the request to determine whether an online alias would serve a valid law enforcement purpose. The work unit supervisor must maintain the requests for online alias and their status (approved/denied) for two years from the date of deactivation of the online alias.

(d) Community Response Division personnel with an approved online alias may use their online alias to make false representations in concealment of personal identity in order to establish social media accounts (i.e. a Facebook account). The establishment of a social media account with an approved online alias must be documented.

9. Authorization for Online Undercover Activity

(a) A sworn officer who has an authorized online alias may also request authorization to engage in online undercover activity. Only sworn officers will be authorized to engage in online undercover activity utilizing the online alias.

(b) Online undercover activity occurs when the officer utilizing the online alias interacts with a person via social media. Online undercover operations will only be utilized when there is reason to believe that criminal offenses have been, will be or are being committed (e.g. internet chat rooms where child exploitation occurs).

(c) Employees must submit a request to engage in online undercover activity. The request must contain the following information:

1) Online alias(es) to be used in the online undercover activity;

2) Social media accounts utilized;

3) Valid law enforcement purpose; and

4) Anticipated duration for the online undercover activity.

(d) The CRD Commander must evaluate the request to determine whether online undercover activity is appropriate. If the request is approved, the authorization must be maintained in the file containing the record of the online undercover activity.

(e) In situations involving exigent circumstances, the CRD Commander supervisor may provide verbal authorization for online undercover activity. The CRD Commander should provide written documentation of the request, the exigent circumstances, and the circumstances of the verbal authorization as soon as practical.

(f) Online undercover activity records will be maintained in the related investigative case file. A record will be maintained of all online undercover activity.

(g) Once authorized to engage in online undercover activity, the officer should utilize the appropriate de-confliction system.

(h) All approved online undercover activity requests will be reviewed monthly by the CRD Commander to ensure continued need for the online undercover activity.

(i) For any alias or online undercover activity that is terminated, a summary will be placed in the file indicating the date of termination of the online undercover activity.

10. Authorization to Utilize Social Media Monitoring Tools

(a) Prior to utilizing a social media monitoring tool, the CRD Commander will submit a request through the chain of command to the Police Major for authorization to use the social media monitoring tool. The social media monitoring tool may be utilized in criminal investigations; criminal intelligence development; and crime analysis and situational assessment reports (e.g. during sporting events, demonstrations or other large gatherings that require a law enforcement presence to ensure the safety of the public). The request must contain the following:

1) A description of the social media monitoring tool;

2) Its purpose and intended use;

3) The social media websites the tool will access;

4) Whether the tool is accessing information in the public domain or information protected by privacy settings; and

5) Whether information will be retained by the Department and if so, the applicable retention period for such information.

(b) The request must be reviewed by the Chief of Police prior to approval.

(c) In exigent circumstances, the work unit supervisor may obtain verbal authorization to utilize the social media monitoring tool and provide written documentation as soon as practical. The written documentation should include a description of the exigent circumstances and the verbal authorization, as well as the required information for the request.

(d) If approved, the social media monitoring tool may be utilized for a period of ninety (90) days or, in the case of situational assessments such as an event or large gathering, until the conclusion of the law enforcement activity related to the event. After ninety (90)

days, the CRD Commander must submit a summary describing the law enforcement actions that resulted from the use of the social media monitoring tool. If continued use is needed, the summary may also contain a request to continue using the social media monitoring tool. The process to approve the request is the same as the original request.

11. Source Reliability and Content Validity

(a) 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.

12. Documentation and Retention

(a) Other than crime analysis and situational assessment reports, all information obtained from social media websites shall be placed within a case file, suspicious activity report, or intelligence report. At no time should Department personnel maintain any social media files outside of these authorized files.

(b) Crime analysis and situational assessment reports may be prepared for special events management, including First Amendment-protected activities. At the conclusion of the situation requiring the report or First Amendment-protected event where there was no criminal activity related to the information gathered, the information obtained from the social media monitoring tool will be retained for no more than fourteen (14) days. Information from the social media monitoring tool that does indicate a criminal nexus will be retained in an intelligence report, suspicious activity report, or case investigative file as directed by the State of North Carolina retention schedule.

(c) Information identified as criminal in nature that is obtained in the course of an investigation from a social media site will be collected and retained using screen shots, printouts of chat logs, copying uniform resource locators (URL's) for subpoena or investigatory purposes, or storing the information via secure digital means. When possible, employees will utilize investigative computer systems and software intended to record data from social media sites.

13. Off Duty Conduct

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

(b) As soon as practical following awareness of the potential criminal activity, the employee should prepare detailed notes to document a complete description of the information observed and specifics as to the events that occurred or action taken.

(c) Employees shall act to preserve and maintain proper custody of images, texts, photographs, or other potential evidence.

(d) Given the ease with which information can be gathered from public internet searches, tracking services, and other computer analytic technology, the use of employee's personal or family internet accounts, social media, or internet service for official Department business is prohibited.

14. Dissemination

(a) 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.

15. Employment Background Investigations

(a) As part of its employment background process, Department personnel will conduct a search of social media websites and profiles in the public domain regarding the applicant. Applicants will be notified that this search will be conducted. Applicants may disclose passwords to social media sites or profiles to the Department, however it is not required. In the event an applicant discloses their password, the Department may use the password to log into the applicant's social media site or profile. Employees will not search or attempt to gain access to private social media profiles.

(b) All searches of applicant social media pages and profiles will only search information that is in the public domain.

(c) Online aliases will not be used to conduct employment background investigations.

(d) Only criminal comments or images will be collected as part of the background investigatory process. Employees will not collect or maintain information about the political, religious, or social views, associations or activities of any individual or any group unless such information directly relates to criminal conduct or activity.

(e) During the course of a background investigation, if a reference, supervisor, or colleague of the applicant provides negative information on the applicant related to a social media site, the investigating officer will prepare an investigative summary outlining the information provided by the reference.

16. Sanctions for Misuse

(a) Any employee who violates the provisions of this directive will be subject to disciplinary action, up to and including termination.

G. PERSONAL USE OF SOCIAL MEDIA

1. Barring state law or binding employment contracts to the contrary, Department personnel shall abide by the following when using social media.

(a) Employees are prohibited from accessing social networking sites while on-duty except in the course of official investigations, or as part of their official job duties, and then only with supervisory approval. In addition, employees shall not access social networking sites from HPD owned computers, laptops, or equipment, except as noted above.

(b) Department personnel are free to express themselves as private citizens on social media sites to the degree that their speech does not impair working relationships of this department for which loyalty and confidentiality are important, impede the performance of

duties, impair discipline and harmony among coworkers, or negatively affect the public perception of the Department.

(c) As public employees, department personnel are cautioned that speech on- or off-duty, made pursuant to their official duties—that is, 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 department. Department personnel should assume that their speech and related activity on social media sites will reflect upon their office and this department.

(d) Employees should expect that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the HPD at any time without prior notice.

(e) Any individual who can be identified as an employee of the Huntersville Police Department has no reasonable expectation of privacy when social networking online, and is subject to all HPD policies, and all local, state, and federal laws regarding public information on arrests, investigations, and personal data. Department personnel shall not post, transmit, or otherwise disseminate any information to which they have access as a result of their employment without written permission from the Chief of Police or his or her designee.

(f) For safety and security reasons, department personnel are cautioned not to disclose their employment with this department nor shall they post information pertaining to any other member of the department without their permission. As such, department personnel are cautioned not to do the following:

1) Display department logos, uniforms, or similar identifying items on personal web pages.

2) Post personal photographs or provide similar means of personal recognition that may cause them to be identified as a police officer of this department. Officers who are, or who may reasonably be expected to work in undercover operations, shall not post any form of visual or personal identification.

(g) Employees should not jeopardize their personal confidentiality and/or that of other employees by posting photographs or personal information about themselves or other members of the HPD.

(h) When using social media, department personnel should be mindful that their speech becomes part of the worldwide electronic domain. Therefore, adherence to the department's code of conduct is required in the personal use of social media. In particular, department personnel are prohibited from the following:

1) Employees shall not post any material that is violent, sexually explicit, racially or ethnically derogatory, discredits or tarnishes the image of the HPD, individuals within the HPD, the town of Huntersville, or show a negative bias to one race, religion, or any protected class of individuals. This restriction shall not prohibit any posting of material that is legitimate public speech involving a matter of genuine public concern.

2) Speech involving themselves or other department personnel reflecting behavior that would reasonably be considered reckless or irresponsible.

3) Engaging in prohibited speech noted herein, may provide grounds for undermining or impeaching an officer's testimony in criminal proceedings. Department

personnel thus sanctioned are subject to discipline up to and including termination of office.

4) All pictures, audio or video recorded, collected, captured, or stored by an employee during an employee's tour of duty, which is related to any official business of the HPD and/or specifically the employee's duty, is the property of the HPD whether the employee utilizes departmental equipment or equipment owned by the employee or another person. Employees shall not post or release photographs, video images, audio files, or text documents that relate to specific HPD case sensitive related work activities (crime scenes, photos depicting potential evidence, reports, etc.) without the express written permission of the Chief of Police.

5) Department personnel may not divulge information gained by reason of their authority; make any statements, speeches, appearances, and endorsements; or publish materials that could reasonably be considered to represent the views or positions of this department without express authorization.

2. Department personnel should be aware that they may be subject to civil litigation for:

   (a) Publishing or posting false information that harms the reputation of another person, group, or organization (defamation);

   (b) 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;

   (c) Using someone else's name, likeness, or other personal attributes without that person's permission for an exploitative purpose; or

   (d) Publishing the creative work of another, trademarks, or certain confidential business information without the permission of the owner.

3. Department personnel should be aware that privacy settings and social media sites are constantly in flux, and they should never assume that personal information posted on such sites is protected.

4. Department personnel should expect that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the Department at any time without prior notice.

5. Employees should be aware that the content of these social networking sites can be subpoenaed and used in criminal and civil trials to impeach the employee's testimony.

H. REPORTING VIOLATIONS

1. Any employee becoming aware of or having knowledge of a posting or of any website or web page in violation of the provision of this policy shall notify his or her supervisor immediately for follow-up action. Employees who violate the provisions of this policy are subject to disciplinary action, up to an including termination.

By Order of:

Cleveland L. Spruill, Chief of Police