BLOOMINGTON POLICE DEPARTMENT

STANDARD OPERATING PROCEDURE

SOCIAL MEDIA

Reviewed by:	Jack McQueen	Effective Date:	December 20, 2019
Authorized by:	Interim Chief Greg Scott	Revision Date:	May 3, 2021

PURPOSE

The 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.

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.

DEFINITIONS

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."

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

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

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

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, Instagram), microblogging sites (Twitter,Nixle), photo and video sharing sites (YouTube, SnapChat, TikTok), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).

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

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

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

POSSIBLE USES BY THE DEPARTMENT

1. Social media is a valuable investigative tool when seeking evidence or information about
    a. Missing persons
    b. Wanted persons
    c. Persons of interest and/or suspects in investigations
    d. Gang participation
    e. Crimes perpetrated online or driven by online activity (i.e., cyber bullying, cyber stalking)
    f. 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
    d. Soliciting tips about unsolved crimes
3. Social media can be used to make time-sensitive notifications related to
    a. Road closures
    b. Special events
    c. Weather emergencies
    d. Missing or endangered persons

MANAGEMENT OF DEPARTMENTAL SOCIAL MEDIA PLATFORMS

1. Determine strategy
    a. 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.
    b. Where possible, the page(s) should link to the department's official website.
2. Procedures
    a. Creation and management of 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 Public Information Officer or as otherwise determined.
        1. During situations involving exigent circumstances (accident related road closures, special events, major incident responses, weather emergencies, and missing persons) an on-duty member of the command staff may post to departmental social media platforms using the GovDelivery system.
        2. The CIAU supervisor or his/her designee may create and manage departmental social media postings related to the solicitation of investigative leads in regard to active criminal investigations. These posts may include text, photographs and/or video production. Posts of this nature may also include the sharing of other law enforcement agency posts regarding solicitation of leads in investigations by external agencies.

b. Social media content shall adhere to applicable laws, regulations, and policies, including all information technology and records management policies.
    1. In compliance with Illinois law (5 ILCS 140/2.15), departmental personnel are prohibited from publishing booking photographs, commonly known as "mugshots", on our social media platforms in connection with civil offenses, petty offenses, business offenses, Class B or Class C misdemeanors unless the posting of the booking photograph is done to assist in the search for a missing person. Posts related to arrestees should always include the following verbiage: "All subjects should be presumed innocent until otherwise proven guilty in a court of law".
c. Where possible, social media pages shall clearly indicate they are maintained by the department and shall have department contact information prominently displayed. All departmental social media sites should display a message indicating that the site(s) are not monitored 24 hours a day.
d. Content is subject to all public records laws (Federal and State FOIA). The Information Technology department is responsible for all digital archival of departmental postings to social media platforms. Requests for archived records should be directed to the City Clerk and Information Technology.
e. Content shall not reveal the private or confidential information of the City, any City employee or any third party.

EMPLOYEES SANCTIONED TO POST TO DEPARTMENTAL PLATFORMS

Department personnel representing the department via social media platforms as part of their work responsibilities shall do the following:

1. 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.
2. Identify themselves as a member of the department.
3. 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 consent of the affected employees.
4. Not conduct political activities or private business.
5. Not utilize personally owned devices to manage the department's social media activities without prior permission from the Chief of Police or his/her designee.
6. Observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic social media.

DEPARTMENT SOCIAL MEDIA PLATFORM LEGAL DISCLAIMER

Where possible, social media pages should contain a written disclaimer that reads as follows:

DISCLAIMER:
The Bloomington Police Department uses social media to learn about communities needs and concerns, contribute to relevant conversations, and promote department programs and services. Despite efforts to keep the department-provided information timely and accurate, users should be aware that the information available through this social media tool may not be timely, accurate, or complete. No communication to the Bloomington Police

Department through this social media shall be deemed to constitute legal or official notice for any purpose. The Bloomington Police Department disclaims any responsibility or liability for positions taken by individuals or entities in their individual cases for any misstatement, misunderstanding and losses, directly or indirectly, on the part of the users.

The Bloomington Police Department's use of external social media tools is provided as a public service. The Bloomington Police Department disclaims liability for ads, videos, promoted content or comments accessible from any external web page. The responsibility of external content or comments rests with the organizations or individuals providing them. Any inclusion of external content or comments on external social media web sites does not imply endorsement by the Bloomington Police Department. We reserve the right to remove comments/materials from the Bloomington Police Department's social media tools when those comments/materials, in the department's sole discretion, are:

- *Potentially libelous, obscene or sexually explicit comments or photos*
- *Personal attacks, insults, profane, or threatening language*
- *Plagiarized material that potentially violates intellectual property rights*
- *Private, personal information published without consent*
- *Commercial promotions or spam*
- *Off topic or that link to material that is off topic*
- *Embedded images from external sources*
- *Violate any law or promote the violation of any law*
- *Encourage or constitute prohibited discriminatory or harassing conduct*
- *Made by a person masquerading as someone else*

Additionally, the Bloomington Police Department reserves the right to terminate a person's ability to post comments/materials or otherwise participate in the department's social media tools when the person has repeatedly posted any of the above listed inappropriate comments/materials. Any person or persons identified on this site as an arrestee or defendant in a criminal case is presumed innocent until proven guilty in a court of law.

When possible, comments or posts that meet the above requirements for removal should be deleted or hidden on any departmental social media sites by the PIO or CIAU Supervisor.

DEPARTMENTAL INVESTIGATIVE USE OF SOCIAL MEDIA

1. The monitoring of social media for investigative purposes should only take place when an officer/employee has articulable and documented criminal predicate on the subject(s) being monitored. Officers/employees cannot collect or capture social media information related to political, religious or social views, associates or activities by any individual group, corporation, business or party unless the information directly pertains to criminal conduct. Officer/employees can not collect or capture information related to 1st Amendment activity, unless the expressive activity is criminal in nature. The requirements of 28 CFR Part 23 should be followed regarding storage and retention of all information, whether collected from social media sites or other information sources.
2. Employee use of personally owned devices or personal social media accounts to conduct social media investigations in the course of official duties is prohibited without prior permission from the Chief of Police or his/her designee.

a. Off duty personnel who happen to obtain social media information they would regard evidentiary, actionable, or intelligence from social media sites shall report this information to appropriate on-duty supervisor and to the Crime and Intelligence Analysis Unit. If the information needs immediate action the supervisor should do so.
b. Off duty personnel are prohibited from creating undercover accounts or otherwise searching for information for the purpose of completing any level of criminal investigations.

3. For the documentation, storage, and retention requirements of information obtained from social media sites that is being utilized for a criminal investigation, information should be maintained as evidence in the criminal case consistent with applicable laws, regulations, and department policies regarding investigations and dissemination or storage of sensitive information.
4. Approved levels of investigative use:
    a. Apparent/Overt Use - In the Apparent/Overt Use engagement level, employee identification need not be concealed. Within this engagement level, there is no interaction between the employee and the subject/group. Information accessed via this level is open to the public (anyone with Internet access can use a public search engine and "see" the information). Accessing this type of social media information would not require a user to log-in to a social media app/site to conduct a search. An example of Apparent/Overt Use would be an employee searching Twitter for any indication of a criminal-related flash mob to develop a situational awareness report for the jurisdiction. Apparent/Overt Use is based on user profiles/user pages being unlocked or open source. For instance, if an employee utilizes a *department owned electronic device* to search for a criminal subject's social media account and determines that a profile which appears to be that of the subject has the account privacy settings set to "public," then the use of that identifying account information would be considered Apparent/Overt Use. The authorization level for Apparent/Overt Use may be minimal, as this level of engagement is considered part of normal, authorized law enforcement investigative activity.
    b. Discrete Use - During the Discrete Use engagement level, the employee's identity is not overtly apparent. There is no direct interaction with subjects or groups; rather, activity at this level is focused on criminal intelligence gathering. An example of Discrete Use is that of an employee utilizing a nongovernmental IP address to read a blog written by a known violent extremist who regularly makes threats against the government. Suspects may use an analytical tool that tracks accesses to his/her blog and that tool may produce identification of the visitor's IP address, agency and/or computers used to access the blog. This identification could potentially identify law enforcement personnel to the suspect leading to a compromised investigation or future safety issues for law enforcement employees.
    c. Covert Use - During the Covert Use engagement level, employees' identity is explicitly concealed. Under Illinois Right of Publicity Act (765 ILCS 1075/), the authorized employee, while utilizing an undercover account, shall not portray their online identity by using photograph(s) or video(s) of other employees or citizens without that employee or citizen's written consent. Employees are engaging in authorized undercover activities for an articulated investigative purpose, and the concealment of the employee's identity is essential. Only those employees approved

for Covert Use of Social Media by either the Lieutenant of the Criminal Investigation Unit or the Lieutenant of the Street Crimes Unit may utilize a covert social media account.

i. Anyone approved for Discrete or Covert Use must first undergo training in regard to undercover use of social media. Training materials can be found on PowerDMS. Unless approved by their supervisor, employees approved to use undercover accounts shall not utilize the undercover account(s) while off-duty. Employees covert uses could include but are not limited to:
    a. The creation of an undercover profile to directly interact with an identified criminal subject online.
    b. Lawfully intercepting information from a social media site, through a court order, as a part of authorized law enforcement action.

EMPLOYEES PERSONAL USE OF SOCIAL MEDIA

Precautions and Prohibitions

Barring any state law to the contrary, department personnel shall abide by the following when using social media.

1. 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. However, nothing within this policy shall limit in any way an employee's right to engage in protected concerted activity under the Illinois Public Labor Relations Act.
2. 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.
3. 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 provided; however, that nothing within this policy shall limit in any way an employee's right to engage in protected concerted activity under the Illinois Public Labor Relations Act.
4. For safety and security reasons, department personnel are urged to exercise the utmost caution before disclosing their employment with this department. Employees shall not post information pertaining to any other member of the department without their permission. As such it is recommended that department personnel exercise caution before they do the following:
    a. Display department logos, uniforms, or similar identifying items on personal social media sites or systems.
    b. 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 undercover operations, should not post any form of visual or personal identification.

5. 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:
    a. Speech containing obscene or sexually explicit language, images, or acts and statements or other forms of speech that ridicule, malign, disparage, or otherwise express bias against any race, any religion, or any protected class of individuals.
    b. Speech involving themselves or other department personnel reflecting behavior that would reasonably be considered reckless or irresponsible.
    c. Weaponry, whether owned by this department and/or owned personally or privately, shall not be displayed or referenced to in any multimedia format, on social media or social net-working sites if such displays or depictions promote or glorify violence.
6. 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.
7. 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. Nothing within this section shall be construed as a limitation on an employee's right to report misconduct pursuant to any state, local or federal Whistleblower law.
8. 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.
9. 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.
10. Department personnel should expect that any information created, transmitted, downloaded, exchanged or discussed in an open or publicly available forum, system or social networking site may be accessed by the department at any time without prior notice.

REPORTING VIOLATIONS

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.