# Social Media - Investigative Use

Eff. Date 1/23/2024

## Purpose

The Madison Police Department (MPD) endorses the use of web-based and mobile-based technologies designed to facilitate internet communications, known as "social media," for the purpose of investigating criminal activities and actors and for the purpose of monitoring any potential or ongoing "flash mobs," protests, riots, or other mass demonstrations. This procedure establishes a standard of conduct in regard to the use of these forms of technology and communication for investigative purposes.

## Application

This procedure applies to all MPD employees and personnel using or posting to social media as an investigative tool during the course of an investigative operation or assignment.

## 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.

***Crime Analysis and Situational Assessment Reports***: Analytic activities to enable MPD to identify and understand trends, causes, and potential indicia of criminal activity.

***Criminal Intelligence Information**:* Data 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.

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

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

***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. This includes sending personal messages to other users or posting content on the timeline of

other profiles. The act of simply joining an online group or sending or accepting a friend request would not be considered undercover activity unless messaging content accompanies said actions.

***Public Domain***: Any Internet resource that is open and available to anyone.

***Social networking websites / social media website****:* 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, X (formerly known as Twitter)), micro blogging sites (Tumblr, Nixle), photo and video-sharing sites (Flickr, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit) where users can create profiles, share information, and socialize with others using a range of technologies. The absence of an explicit reference to a specific social media website does not limit the application of this policy.

***Valid law enforcement purpose***: Investigation or information/intelligence-gathering development, collection, use, retention or sharing that furthers the authorized functions and activities of a law enforcement agency – which may include prevention of crime, ensuring the safety of the public and public or private structures and property, and/or furthering officer safety (including situational awareness) and homeland and national security – while adhering to law and agency policy designed to protect the privacy, civil rights, and civil liberties of Americans.

**Procedure**

This procedure serves to clarify and establish guidelines and prohibitions for MPD-authorized use of social media for investigative purposes. These guidelines and prohibitions build on policy requirements put forth in the Law Enforcement Code of Ethics, MPD Mission Statement and Core Values, MPD Code of Conduct and Standard Operating Procedures, City of Madison Administrative Procedure Memoranda (APM), as well as established City, State, and Federal Law. However, because investigations utilizing social media may involve undercover or confidential activities, requiring a certain level of dissimulation and clandestinity, portions of these requirements (specifically those put forth in APM 3-16 and MPD Code of Conduct and Standard Operating Procedures) may not be universally applicable to actions taken during such investigations.

Social media as an investigative tool may be used by members of MPD for a valid law enforcement purpose consistent with this SOP. Unless such information is relevant to the individual or if the individual or organization is involved in an activity or event that may require advanced notice in order to coordinate adequate police resources to ensure public safety, maintain order, or protect property, the employee will not utilize social media to seek or retain information about the following:

1. Individuals or organizations solely on the basis of their religious, political, or social views or activities
2. An individual or organization's participation in a particular non-criminal organization or lawful event
3. An individual's race, ethnicity, citizenship, place of origin, disability, gender, or sexual orientation
4. An individual's age other than to determine if someone is a minor

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.

No authorization is necessary to access information available in the public domain, so long as the access is consistent with this SOP. The use of personal social media accounts for investigations is discouraged.

**Online Alias**

Sworn officers, analysts, or authorized police department personnel may only use an online alias to seek information for a valid law enforcement purpose. Only sworn officers and analysts are authorized to create an online alias. The employee seeking authorization to create/utilize an online alias will complete the MPD online alias request form and submit it to their commanding officer for approval. The commander will review the request and determine whether use of the online alias would serve a valid law enforcement purpose. If exigent circumstances require the immediate creation of an online alias without prior approval, the employee will notify their commanding officer of the online alias creation as soon as possible. Within a reasonable amount of time following the exigent circumstance, the employee will document the online alias. The employee will include all the information that would have been documented on a request form.

A. When necessary, profile pictures or website images of humans purporting to depict the operator of the alias profile must be of an individual over the age of 18 who has provided written consent for the image to be used.

B. Online alias usernames and passwords shall be made immediately available to supervisors upon request.

C. Alias accounts should only be used with Department-issued devices while on duty, unless otherwise approved by a supervisor.

**Online Undercover Activity**

Only sworn officers may engage in online undercover activity with command approval. The officer seeking authorization to engage in online undercover activity will complete the MPD online undercover activity request form and submit it to their commanding officer. The commanding officer will review the request and determine whether the online undercover activity serves a valid law enforcement purpose. If exigent circumstances require the immediate use of online undercover activity without prior approval, the employee will notify their commanding officer of the online undercover activity as soon as possible. Within a reasonable amount of time following the exigent circumstance, the officer will document the online undercover activity. The employee will include all the information that would have been documented on a request form.

A. When necessary, profile pictures or website images of humans purporting to depict the operator of the alias profile must be of an individual over the age of 18 who has provided written consent for the image to be used.

B. Online alias usernames and passwords shall be made immediately available to supervisors upon request.

C. Undercover work should only be performed with Department-issued devices while on duty, unless otherwise approved by a supervisor.
D. For Internet Crimes Against Children (ICAC)-related online undercover investigations, those investigations must also conform to the ICAC Program Operational and Investigative Standards Manual.

All online undercover activity yielding actionable intelligence or leading to the development of probable cause will be documented. The commanding officer will regularly review all online undercover activity requests to ensure a continued need for the online undercover activity.

**Real Time and Open Source Analysis Tool**

Employees may use social media monitoring tools that gather information from the public domain only for a valid law enforcement purpose. Employees may only use social media monitoring tools that gather information not within the public domain with command approval. The commanding officer will review the request and determine whether the use of social media monitoring tools is appropriate. If exigent circumstances require the immediate use of social media monitoring tools (that gather information not within the public domain) without prior approval, the employee will notify their commanding officer as soon as possible. Within a reasonable amount of time following the exigent circumstance, the officer will document the use of the monitoring tool.

**Documentation**

Documentation of command approval will occur electronically through the MPD SharePoint site, unless an exception has been approved by the Chief.

Employees should place any relevant case information obtained from social media websites within a Law Enforcement Records Management System (LERMS) case file, suspicious activity report, police report, or intelligence bulletin. MPD personnel will not maintain any social media files/records outside of these authorized files.

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, the information obtained that indicates a criminal nexus will be retained in an intelligence bulletin, suspicious activity report, police report, or LERMS case file as directed by the established retention schedule.

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

At no time should the name of an individual or organization that is not reasonably suspected of criminal activity be recorded unless such name is clearly labeled as “non-criminal identifying information.”

**Dissemination**

Information recorded in accordance with this SOP will only be disseminated when authorized by the Records Custodian and the Office of the City Attorney.

**Audit**

Compliance with this SOP will be verified as part of case management meetings with employees.

Original SOP: 02/25/2015
(Revised: 02/05/2016, 03/26/2018, 05/02/2018, 1/23/2024)
(Reviewed Only: 11/01/2016, 01/31/2020, 02/04/2022)