NENA Standard for Social Media Emergency Requests

Abstract: This document is provided to assist Public Safety Answering Points (PSAPs) in establishing standards in the handling of emergency requests for public safety assistance that originate on social media networks and interacting with providers for exigent circumstances.

NENA Standard for Social Media Emergency Requests

NENA-STA-044.1-2022
DSC Approval: 03/22/2022
PRC Approval: 05/06/2022
NENA Board of Directors Approval: 05/19/2022
Next Scheduled Review Date: 05/19/2025

Prepared by:
National Emergency Number Association (NENA) PSAP Operations Committee, Social Media Emergency Requests Working Group

Published by NENA
Printed in USA

1 Executive Overview

The abundant availability of Internet access and increasing development of websites and smart phone applications available to the public that allow individuals to quickly communicate information about themselves in a digital world has transformed how society communicates. These technologies, defined as part of Web 2.0 (includes Twitter, Facebook, and other social media sites and widgets), have created methods of communicating that are quickly becoming a primary method of communicating between individuals, especially in specific demographics such as teenagers. Social media is quickly becoming the predominant method of keeping individuals informed about a variety of current events on both a personal level as well as events in global community. The popularity of social media applications has been facilitated by the offering of numerous free or low-cost applications and the mobility provided to consumers through smart phones. This has created a phenomenon where the public may be made aware of a public safety incident prior to the first 9-1-1 call being received at the Public Safety Answering Point (PSAP) to report the emergency.

Social media provides individuals with an efficient platform for communicating with large numbers of people expeditiously. Similarly, a PSAP may find information to post that will reduce incoming inquiry phone calls. Posting information such as accidents blocking a roadway; events that spur media interest and other real time information allows users to refer to the social media site instead of calling into the PSAP. Some forms of social media also allow for location specific information to be broadcast, commonly known as "checking in."

Critical incidents, such as college campus shootings and natural disasters, have demonstrated that public service entities must adapt to this technology and incorporate social media into their operations. In addition, postings by individuals requesting police, fire, or emergency medical service assistance have grown in frequency necessitating the implementation of policies to guide PSAP usage in monitoring social media. Each PSAP must also include policies on how to effectively respond to secondhand requests for assistance that are prompted by postings on social networks.

PSAPs must review all "Terms" that are posted by social media sites. PSAPs should be aware of what information, photos, and videos are retained by the social media site owners. Some social media sites claim property rights to all media once posted. Each PSAP should develop a policy outlining what is acceptable material that can be posted to a social media site, but on an agency's official social sites as well as employees' sites to ensure that critical public safety information is not inappropriately released through social media.

When considering social media policies, procedures and/or guidelines, PSAPs should ensure that their policies are not in conflict with any current local, county, state, and/or federal statutes or requirements. PSAPs should consult with agency legal team or solicitor before launching a social media site.

Table of Contents

1 EXECUTIVE OVERVIEW 2

DOCUMENT TERMINOLOGY 5

INTELLECTUAL PROPERTY RIGHTS (IPR) POLICY 6

REASON FOR ISSUE/REISSUE 6

2 SOCIAL MEDIA USE BY PSAPS 7

2.1 PSAP OPERATIONS 7
2.2 COMMUNICATING WITH SOCIAL MEDIA PROVIDERS 10
2.3 PUBLIC EDUCATION/INFORMATION 11
2.4 HUMAN RESOURCES 11
2.5 PSAP TRAINING 12
2.6 CONTINGENCY PLANNING 12

3 NENA REGISTRY SYSTEM (NRS) CONSIDERATIONS 12

4 DOCUMENTATION REQUIRED FOR THE DEVELOPMENT OF A NENA XML SCHEMA 12

5 IMPACTS, CONSIDERATIONS, ABBREVIATIONS, TERMS, AND DEFINITIONS 13

5.1 OPERATIONS IMPACTS SUMMARY 13
5.2 TECHNICAL IMPACTS SUMMARY 13
5.3 SECURITY IMPACTS SUMMARY 14
5.4 RECOMMENDATION FOR ADDITIONAL DEVELOPMENT WORK 14
5.5 ANTICIPATED TIMELINE 15
5.6 COST FACTORS 15
5.7 COST RECOVERY CONSIDERATIONS 15
5.8 ADDITIONAL IMPACTS (NON-COST RELATED) 15
5.9 ABBREVIATIONS, TERMS, AND DEFINITIONS 16

6 RECOMMENDED READING AND REFERENCES 17

7 EXHIBIT A 18

EMERGENCY DISCLOSURE REQUEST 18

APPENDIX A – SOCIAL MEDIA PROVIDERS 19

APPENDIX B – STANDARD OPERATING PROCEDURE TEMPLATE 21

ACKNOWLEDGEMENTS 24

NENA
STANDARD DOCUMENT
NOTICE

This Standard Document (STA) is published by the National Emergency Number Association (NENA) as an information source for 9-1-1 System Service Providers, network interface vendors, system vendors, telecommunication service providers, and 9-1-1 Authorities. As an industry Standard it provides for interoperability among systems and services adopting and conforming to its specifications.

NENA reserves the right to revise this Standard Document for any reason including, but not limited to:

- Conformity with criteria or standards promulgated by various agencies,
- Utilization of advances in the state of the technical arts,
- Reflecting changes in the design of equipment, network interfaces, or services described herein.

This document is an information source for the voluntary use of communication centers. It is not intended to be a complete operational directive.

It is possible that certain advances in technology or changes in governmental regulations will precede these revisions. All NENA documents are subject to change as technology or other influencing factors change. Therefore, this NENA document should not be the only source of information used. NENA recommends that readers contact their 9-1-1 System Service Provider (9-1-1 SSP) representative to ensure compatibility with the 9-1-1 network, and their legal counsel, to ensure compliance with current regulations.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license is granted, whether expressed or implied. This document shall not be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA, or any affiliate thereof, to purchase any product, whether or not it provides the described characteristics.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA's Committees have developed this document. Recommendations for changes to this document may be submitted to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

NENA: The 9-1-1 Association improves 9-1-1 through research, standards development, training, education, outreach, and advocacy. Our vision is a public made safer and more secure through universally available state-of-the-art 9-1-1 systems and better-trained 9-1-1 professionals. Learn more at nena.org.

Document Terminology

This section defines keywords, as they should be interpreted in NENA documents. The form of emphasis (UPPER CASE) shall be consistent and exclusive throughout the document. Any of these words used in lower case and not emphasized do not have special significance beyond normal usage.

1. MUST, SHALL, REQUIRED: These terms mean that the definition is a normative (absolute) requirement of the specification.
2. MUST NOT: This phrase, or the phrase "SHALL NOT," means that the definition is an absolute prohibition of the specification.
3. SHOULD: This word, or the adjective "RECOMMENDED," means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behavior described with this label.
5. MAY: This word, or the adjective "OPTIONAL," means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option "must" be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option "must" be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

These definitions are based on IETF RFC 2119 [2].

Intellectual Property Rights (IPR) Policy

NOTE – The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, NENA takes no position with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from NENA by contacting the Committee Resource Manager identified on NENA's website at www.nena.org/ipr.

Consistent with the NENA IPR Policy, available at www.nena.org/ipr, NENA invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard.

Please address the information to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

Reason for Issue/Reissue

NENA reserves the right to modify this document. Upon revision, the reason(s) will be provided in the table below.

Document Number	Approval Date	Reason For Issue/Reissue
NENA-STA-044.1-2022	05/19/2025	Initial Document

2 Social Media Use by PSAPS

2.1 PSAP Operations

Prior to any implementation of social media by a PSAP, policies and procedures should be developed that clearly define the role of social media, restrictions on its usage, and expectations of employee behavior. Written policies should clearly define that any criminal justice or medical information, including documents or photos, related to the agency's operations or its employees' privileged information is strictly prohibited and could pose a liability threat to the agency and potential damage any ongoing investigations.

A PSAP that regularly utilizes social media as part of their normal communications should take into consideration if the additional workload provides justification for additional staffing. If social media is proactively utilized to keep the public informed, i.e., tweeting vehicle accidents or road closures, a PSAP may need to consider specific position assignments for this task and those personnel who are authorized to perform this function.

There will inevitably be requests for service posted to a social media site. PSAPs SHOULD have policies and procedures guiding dispatchers on how to handle these requests is they are observed by PSAP personnel or they are made aware of them by a 3rd party source. PSAPs will need to consider what priority should be given to the requests in relation to other incoming requests, such as telephone calls routed through a 9-1-1 network.

If a PSAP receives a request for assistance via a social media site, the PSAP telecommunicator SHOULD make an attempt to establish a voice connection with the citizen, if at all possible. There may be some situations where the citizen may be put in danger and unable to call, therefore, the telecommunicator SHALL handle the request as if it were received through the voice network.

There are five (5) scenarios that PSAPs may encounter in dealing with requests for emergency assistance that are posted on social media sites:

A. **Emergency post – no information:** An individual posts a request for help but does not provide any context of the emergency, no information on where the emergency is located or how to make contact with them via telephone.
B. **Emergency post – basic information:** An individual posts a request for help with the minimum information needed to dispatch field responders, such as context of the emergency and location.
C. **Emergency post – outdated information:** An individual posts a request for help, however, a gap in time exists between when the post was made and when the PSAP became aware of the emergency. The PSAP should consider the circumstances of the event(s) to determine what amount of time would be considered significant enough that the information may be outdated. Examples might include a natural disaster where victims may need to be rescued but the PSAP only became aware of

them hours into the event. PSAPs SHOULD have a local policy that includes verifying if the citizen still requires assistance and how to handle incidents that are reported much later after they have occurred.

D. **3rd party notification**: A citizen calls 9-1-1 to report that another individual has posted a request for assistance on a social media site.
E. **Social Media provider contacts PSAP:** A social media provider has identified a potential emergency request for assistance by one of their consumers and contacts the local PSAP directly for response.

If a PSAP receives a request for assistance via a social media site, telecommunicators will need to utilize standard information gathering practices that include, at a minimum:

A. Address or exact location of the incident, if available
B. Telephone number and/or an alternate means of contact such as user identification or email address.
C. Type of emergency
D. Time of occurrence
E. Hazards
F. Identity of individuals involved and their location

Additional information SHOULD be gathered that is specific to the social media post. if available. such as:

A. Social media site that the post was made on, e.g., Facebook, Twitter, etc.
B. Screen name
C. The location of the posting on the social media site, e.g., individual's feed, group page, etc.
D. Any information on the user's social media profile, e.g., location, email address, or telephone number
E. Any information that can be discerned from the social media provider, e.g., IP address, the geo-location of the post, if the user has location services enabled on their device, etc. This information may need to be passed on to another agency for appropriate response.

Non-English-speaking social media requests will occur. The PSAP SHOULD identify resources that are available to interpret written requests. Some examples where translators may be found are internally within your agency, web-based applications, community colleges, universities, and language translation companies. There may be other resources that are available in the PSAP's community.

There may be times where information is made known about a public safety incident that will occur in the future, e.g., planned gang fight, flash mob, etc. PSAPs SHOULD refer to their local policy for handling tips/notifications of potential emergency events that may occur in the future.

Initial call processing techniques utilized by the PSAP should be standardized for all requests for service regardless of the method of origination. However, PSAPs SHOULD train Telecommunicators on their agency's specific policies governing the use of social media to include responding to the public via social media.

The local jurisdiction may operate or have access to a Real-Time Crime Center or Fusion Center that could assist the PSAP in retrieving information from social media providers. Personnel in these centers typically interact with external parties to gather intelligence and may be able to assist the PSAP. During active events, they may already be crowd-sourcing information that will be beneficial to the PSAP in handling requests for service. The PSAP SHOULD have a local policy that covers the sharing of information between the PSAP and these centers for these types of events. This policy may include assigning PSAP personnel to the center temporarily during the event to coordinate information exchange.

PSAPs SHALL be prepared to receive information or requests that may be from the communities with disabilities. Social media must be accessible and usable by persons with disabilities in accordance with Section 508 of the Rehabilitation Act and Section 255 of the Communications Act, as amended. On January 18, 2018, the U.S. Access Board published a final rule updating accessibility requirements for information and communication technology (ICT) covered by Section 508 of the Rehabilitation Act and Section 255 of the Communications Act. PSAPs SHOULD refer to the guidelines and guidance in Section 508 when preparing social media messages to ensure accessibility to the extent that they are supported by the social media provider."

If at all possible, plain English is recommended to ensure that there is no miscommunication. Preparations should include some basic level of understanding of limitations with social media to ensure effective communications, for example, character limitations and messages possibly being broken into multiple messages not delivered in sequential order.

Policies and procedures SHOULD include how social media public safety requests will be handled and under what circumstances. When developing policies and procedures, PSAPs SHOULD consider the following:

- if the PSAP will respond to requests posted on the PSAP's social media site
- when a call is received from a citizen with information about a social media posting
- if the agency will monitor social media sites for key words that would indicate a need for a public safety response

The PSAP should become familiar with GPS-enabled posts to assist in locating citizens requesting assistance. Apps are also available on smart devices that allow the device to be located based on their GPS location. For posts to social sites that do not provide a geographic location of the poster, PSAPs may have other information such as an IP address that could be used to help determine location. PSAPs may need to pass on this information to another agency for an appropriate response. PSAPs may need to contact service providers to obtain additional information in order to dispatch emergency responders. See Exhibit A for a sample emergency disclosure request form that can be utilized to request information from service providers.

PSAPs receiving requests for assistance from a social media site that are not within their own jurisdiction SHALL follow their current policies and procedures for referring calls to other jurisdictions.

PSAPs SHOULD include policies and procedures on how to handle information pertaining to a request for a public safety response after the incident has been completed. Such policies and procedures could include, but are not limited to, considerations for investigative purposes, privacy of the citizen making the request and/or how to capture the information for later use. A disclaimer SHOULD be included on the social media site indicating that everything posted is public information and remains a permanent record of the agency.

If an agency is not going to accept requests for assistance via their social media site, it is recommended that the ability to post be limited to administrators only and/or a disclaimer be placed on the social media site referring the citizen to the PSAP's telephone number.

PSAPs SHOULD routinely perform searches to watch for unauthorized social media sites that falsely identify themselves as representing a PSAP. If such sites are found, the PSAP SHOULD take immediate action to contact the service provider to have the site shut down.

2.2 Communicating with Social Media Providers

PSAPs SHOULD contact social media providers to foster a working relationship with each platform if possible. This will not only help define the needs and capabilities of both the PSAP and social media provider but could also reduce time in the handling of exigent circumstances requests.

PSAPs may need to gather additional information (e.g., screen name, IP address) from a social media post where an emergency response is determined necessary. The request may be initiated by the Telecommunicator or by another agency representative. The telecommunicator may need to contact a social media provider for this information. PSAPs SHALL have a Standard Operating Procedure (SOP) in place that addresses exigent circumstances for emergency requests for service that includes social media providers. The policy SHALL also designate the authority within the agency that can make the request.

It is possible that the social media provider may decide not to release the information to the agency or there could be a delay in when the information is provided. PSAPs SHALL document all responses in the call record.

A sample exigent circumstances form is available in Appendix A of this document.

2.3 Public Education/Information

Social media can be used in unique ways to educate the public, provide up to the minute information. Many agencies are currently using social media to communicate with their communities. Citizens, media groups, and businesses can sign up to "follow," "friend," or "Like" the agency to receive updates and information as it is posted.

PSAPs are able to take advantage of social media in many ways. For example, in the case of an accident, an agency's social media post could assist the units on the scene to reduce traffic, as well as reduce inquiries to the PSAP. Posting current crime trends, wanted persons details, and who to notify in reference to tips provide citizens a venue to gather and provide critical details without having to contact a PSAP. Providing real-time information and updates on local incidents will allow the agencies to immediately broadcast the information to the public.

PSAPs can also use social media to increase engagement with their communities by posting dates, times, and locations of community and in-house events, including but not limited to town hall meetings, safety fair events, and citizens' police academies.

PSAPs SHOULD be familiar with all terms, conditions, and settings prior to setting up a social media site, as well as understand a platform's security settings to configure posts to allow the public to enter posts or comment on an agency's post. It is recommended that PSAPs refer to their local or state laws on digital media. PSAPs SHOULD be aware that censoring (edit, delete, hide, etc.) posts and/or comments may not be possible or allowable by law [3]. It is recommended that all posts be vetted through an appropriate agency approval process to ensure that no protected (e.g., victim details), confidential information (e.g., criminal histories, crime scene photos), or inappropriate content is posted. Information must be relevant and timely, requiring sites to be kept current. Posts must be made often enough to keep the user's interest but not so often that they are inundated with information.

2.4 Human Resources

Using social media for recruiting could potentially widen the applicant pool for PSAPs. Social media is not restricted to the municipality or region when advertising – it is seen worldwide. Posting information informs potential applicants on what to expect when applying for employment with an agency. A common challenge among agencies is the time it takes to put an applicant all the way through a hiring process, from application, testing, background, polygraph, psychological to final interview. Posting anticipated time frames for each step will ready applicants for the extended time the process may take.

An agency maintaining a social media site may allow citizens to post human resource questions to dispatchers. Allowing this to occur as part of a recruiting process would permit potential applicants to better understand the duties of the position. Agencies SHALL identify who has the authority to post to ensure the information is accurate and presents the agency in a positive light.

Dispatchers could answer questions on the roles and responsibilities and other factors that are not always included in a job description, such as working long hours, weekends/holidays, and varied shifts.

Encouraging dispatchers to post what they like most about their position also allows a potential applicant to compare that with what they believe the job to entail. Many times, the perspective of a potential applicant is quite different from the actual job duties and requirements.

Agencies SHOULD consider including a disclaimer advising that the social media site is for informational purposes only. Verbiage SHALL be included to indicate the site is not monitored 24/7 and requests for a public safety response should be made by phone. A legal review SHOULD be done prior to posting information such as the PSAP testing process.

2.5 PSAP Training

A PSAP may use a social media site for posting regional training or sharing of training opportunities and resources. Updates on training classes, APCO and NENA type meetings, and other PSAP related information could be posted for immediate access. The PSAP would need to determine if the site were to be "locked down" to only authorized members.

2.6 Contingency Planning

All social media platforms SHOULD be monitored well in advance of a known event such as severe weather, large-scale social gatherings.

Catastrophic events may create an increase in requests for service as well as the need for posting safety information for the public at-large to the agency's social media site. PSAPs should ensure that personnel are cross trained in the monitoring of social media to handle any increased demand. If applicable, agency contingency plans SHOULD consider a social media component in their communications with the public.

3 NENA Registry System (NRS) Considerations

Not Applicable

4 Documentation Required for the Development of a NENA XML Schema

Not Applicable

5 Impacts, Considerations, Abbreviations, Terms, and Definitions

5.1 Operations Impacts Summary

Each PSAP SHALL determine what role social media serves in their agency's operational and contingency plans. Social media can provide PSAPs with a tool to post feeds, comments, tweets, etc. on social media sites to provide and direct safety and incident information to the public. Social media should be utilized in such a manner that it complements and supports an agency's existing means of disseminating information before, during, and after a public safety incident.

During crisis or disaster situations (i.e., hurricane or ice storm), a PSAP SHOULD augment their public announcement efforts by publishing information such as shelter locations, evacuation routes and food and water distribution to social media sites to ensure a wide dissemination, especially if normal communications methods have been compromised. If an emergency operations plan has been activated, this function may be assigned to a specific individual, such as the PSAP's public information officer. Operations may be impacted by the assignment and/or workload of such duties when such tasks are not conducted during normal operations.

PSAPs SHOULD monitor their agency's social media sites or those of their city or county during a crisis or disaster in the event that a citizen posts critical information such as flooded roadways and tornado sightings. This type of information assists the PSAP in responding to emergencies as well as assisting emergency officials with allocation of resources to affected areas. Telephone networks may become congested during crisis or disaster incidents preventing citizens from contacting emergency services. Citizens may post requests for emergency assistance on an agency's social media site if they are unable to make a telephone call and the agency's site has been configured to receive postings from the public.

PSAP Managers SHALL evaluate the operational impact of implementing the use of social media to respond to requests for service under normal operational circumstances. Social media adds an additional path to handling emergency calls that will impact daily operations. Consideration SHALL be given to the method(s) in how PSAPs monitor and respond to such requests, as well as personnel training and staffing and development of operational policies to accommodate. PSAPs SHALL weigh the impact on operations of allowing or disallowing the use of public comments on the agency's social media posts. Allowing comments will increase the need to monitor the agency's site proactively and respond accordingly.

5.2 Technical Impacts Summary

If applicable, PSAPs SHALL develop an implementation plan that allows employees access to the social media utilized by the PSAP. Firewall access and/or special privileges may need to be available for employees to monitor and post to social media sites. Legacy networks

SHOULD be evaluated to determine the impact of implementing social media to prevent overloading the network.

Implementation of Next Generation 9-1-1 (NG9-1-1) may provide a more seamless implementation of handling requests for service initiated via social media. NG9-1-1 will impact the technology and call flow paths available to PSAPs. PSAP personnel SHOULD monitor the progress of NG9-1-1 adoption and the evolution of the NG9-1-1 standards to determine alternative methods of incorporating the use of social media into a PSAP's normal operations.

5.3 Security Impacts Summary

PSAPs should take into consideration all possible threats and risks involved in the use of social media. In order to monitor or post information on social media sites, it will be necessary for PSAP personnel to access the Internet. This will make PSAP equipment and/or computer networks vulnerable to email phishing, spam, and virus attacks. PSAP administrators SHOULD consider utilizing social media on a workstation that is on a separate network from their critical infrastructure to prevent any such attacks from comprising their emergency operations.

For those agencies who utilize social media as a one-way communications tool with the public (i.e., press releases and announcements), administrators SHALL select specific personnel who will be authorized to post information on behalf of the agency. The PSAP SHALL develop policies as to the type of information that may be posted so that critical or restricted information is not inadvertently released, such as sensitive criminal justice information or details on juvenile victims. Policies SHALL clearly define any approval processes instituted by the agency.

PSAPs should determine if any other entity has created a social media site using the name of the agency. Agencies have found that media and individuals have created social media sites that appear to represent the agency, however, are unauthorized sites. These agencies have found that requiring these unauthorized sites to shut down has been very difficult and time consuming. Social media providers may provide a process that verifies the agency's authenticity. Agencies SHALL work with the social media provider to ensure unofficial accounts are shut down.

5.4 Recommendation for Additional Development Work

There is a need for additional development work to facilitate fully integrating the use of social media communications into a PSAP's operations.

Platform developers SHOULD be encouraged to work with the 9-1-1 community to develop technical interfaces that can share information to 9-1-1 and/or Computer Aided Dispatch systems to aid an agency's response to an incident.

The 9-1-1 community SHOULD identify key contacts with social media providers to facilitate exigent circumstance requests and reduce response times.

Considerations for network bandwidth, network security, and agency permissions need to be addressed if social media is used at a 9-1-1 call taking position.

5.5 Anticipated Timeline

Implementation of this type of endeavor will vary from agency to agency based on their current degree of social media participation. Several basic steps should be considered before heading into the process.

- What is the goal of the agency: hiring, providing real time information, training, intake of emergency requests for service or other topics?
- Which social media platforms(s) will the agency utilize and/or actively monitor?
- Does the agency have a social media policy in place, or does it need to be updated?

5.6 Cost Factors

A PSAP considering the use of social media should consider costs that may be incurred as a result, such as:

- Will current PSAP personnel implement and manage the social media sites, or will contract labor be employed?
- Is additional equipment needed to access social media sites? Will personnel need separate computers to access social media sites so as to not impact critical infrastructure? Is additional software needed to allow for firewall access?
- Does the agency currently have an internet connection? If not, what means will be considered to access the social media sites?
- If multi-media will be included on the social media site, does the agency currently have access to the tools to create presentations (e.g., closed captioning)?
- Advertising on social media sites to promote the PSAP site.

5.7 Cost Recovery Considerations

Normal business practices shall be assumed to be the cost recovery mechanism.

5.8 Additional Impacts (non-cost related)

The information or requirements contained in this NENA document are expected to have 9-1-1 Center operations and 9-1-1 technical impacts. The primary impacts are expected to include:

- Policy and procedure creation and/or updates
- Personnel staffing for managing/monitoring social media networks
- PSAP security for the agency, including but not limited to networks, equipment, and authorized access

5.9 Abbreviations, Terms, and Definitions

See the NENA Knowledge Base for a Glossary of terms and abbreviations used in NENA documents. Abbreviations and terms used in this document are listed below with their definitions.

Term or Abbreviation (Expansion)	Definition / Description
NG9-1-1 (Next Generation 9-1-1)	An IP based system comprised of hardware, software, data, and operational policies and procedures that: (A) provides standardized interfaces from emergency call and message services to support emergency communications; (B) processes all types of emergency calls, including voice, data, and multimedia information; (C) acquires and integrates additional emergency call data useful to call routing and handling; (D) delivers the emergency calls, messages, and data to the appropriate public safety answering point and other appropriate emergency entities; (E) supports data or video communications needs for coordinated incident response and management; and (F) provides broadband service to public safety answering points or other first responder entities. Agreed to by NENA, NASNA, iCERT, and the National 9-1-1 Office representatives on 01/12/2018, see: 47 USC 942: Coordination of 9-1-1, E9-1-1, and Next Generation 9-1-1 implementation Also known as: *Next Generation 9-1-1 Services*
PSAP (Public Safety Answering Point)	An entity responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy.
SOP (Standard Operating Procedure)	A written directive that provides a guideline for carrying out an activity. The guideline may be made mandatory by including terms such as "shall" rather than "should" or "must" rather than "may".

6 Recommended Reading and References

[1] National Emergency Number Association. *NENA Master Glossary of 9-1-1 Terminology*. NENA-ADM-000.24-2021. Arlington, VA: NENA, approved June 22, 2021.

[2] Internet Engineering Task Force. *Key words for use in RFCs to Indicate Requirement Levels*. S. Bradner. RFC 2119, March 1997.

[3] Walden, Andrew. "HPD Ordered to Pay $31K Over Censored Facebook Comments." *Hawai'i Free Press.* June 27, 2014. http://www.hawaiifreepress.com/Articles-Main/ID/12959/HPD-Ordered-to-Pay-31K-over-Censored-Facebook-Comments/.

[4] International Association of Chiefs of Police (IACP). "Technology and Social Media." Last accessed September 26, 2021. https://www.theiacp.org/resources/technology-and-social-media/.

[5] 18 USC 2702: Voluntary Disclosure of Customer Communications or Records. 18 U.S.C. § 2702(b)(8) and § 2702(c)(4). https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2702&num=0&edition=prelim/.

[6] Digital.gov. "Improving the Accessibility of Social Media in Government" Last accessed January 6, 2022. https://digital.gov/resources/improving-the-accessibility-of-social-media-in-government.

7 Exhibit A

EMERGENCY DISCLOSURE REQUEST

ATTN:

This agency requests disclosure of customer information from a user(s) of your service that it has been reported to us that the individual(s) may be experiencing an emergency that warrants the response of police, fire, or emergency medical services. The timely disclosure of such information will ensure that this individual(s)'s health and welfare are not jeopardized due to a delay in retrieving the information.

1. What is the nature of the emergency?

2. Whose person or property is being threatened?

3. What is the imminent nature of the threat?

4. Please explain why the normal disclosure process (including any statutory emergency procedures) would be insufficient or untimely in light of the deadline set forth in Question 3.

5. What specific information in the service provider's possession related to this emergency are you seeking to receive on an emergency basis?

6. How will this information assist in averting the threatened emergency?

I declare under penalty of perjury that the foregoing is true and correct.

______________________________ ___________ ____________________

Printed Name of Officer Badge # Date of Request

Appendix A – Social Media Providers

Name of Platform	Description of Platform	Exigent Circumstance Contact Information
Facebook	Social media app for posts, pictures, videos, live streaming, events, businesses, dating, and gaming	https://www.facebook.com/records/login
Snapchat	Social media app focusing on pictures and videos; also has a user-discretion enabled map displaying "friends'" locations	https://lawenforcement.snapchat.com/en-US/emergency
Instagram	Social media app focusing on pictures, videos, and live streaming	https://www.facebook.com/records/login
Twitter (includes Periscope)	Social media app for brief messages, alerts, and promotions	https://legalrequests.twitter.com/forms/landing_disclaimer
YouTube	Social media app focusing on videos	https://support.google.com/legal-investigations/contact/records
Messenger	Messaging app with video capabilities linked with Facebook	https://www.facebook.com/records/login
WhatsApp	Messaging app with video capabilities; acquired by Facebook in 2014	https://www.whatsapp.com/records/login
Kik	Messaging app with video capabilities	https://medialabai.force.com/KikHelpCenter/s/topiccatalog/law-enforcement
Google (including Gmail & other Google owned platforms)	International company owning Internet related products and collaboration platforms such as calendar, Drive, and email	https://support.google.com/legal-investigations/contact/records

Microsoft (including Xbox Live, OneDrive, Office 365 software)	International company with hardware, software, cloud, and gaming products	Contact corporate offices at 425-882-8080, reference agency case #, and explain problem
PlayStation	Video gaming console featuring interactive and digital entertainment	Will need to call Sony direct: Sony Interactive Entertainment LLC 2207 Bridgepointe Parkway San Mateo, CA 94404 United States of America In the United States and Canada On the web: http://www.playstation.com/support By Phone: 1-800-345-7669 Jennifer Liu General Counsel Senior Vice President, Business and Legal Affairs Tel.: 1-800-345-7669. Fax: 1-310-981-1570 2207 Bridgepointe Parkway San Mateo, California 94404
Apple	International company with hardware, software, and cloud products	https://www.apple.com/legal/privacy/le-emergencyrequest.pdf
Uber	App for peer-to-peer ridesharing, transportation, and food delivery	https://lert.uber.com/s/portal-submission
Lyft	App for peer-to-peer ridesharing, transportation, and food delivery	https://lyft.mailroom.datagov360.com/intake-form
Tinder	Dating app	legaldept@gotinder.com
Grindr	Dating app for gay, bi, and trans persons	https://help.grindr.com/hc/en-us/requests/new?ticket_form_id=126147
TikTok	video-sharing social networking service; intended for ages 13+	https://www.tiktok.com/legal/report/EDR

Appendix B – Standard Operating Procedure Template

The following SOP template is being provided as a baseline document for PSAPs to develop a local policy on the use of social media. PSAPs should substitute the information in brackets with their applicable agency as well as include any specific local policies that are covered by the subject matter. This template is not intended to be a comprehensive document to cover all of a PSAP's specific local laws and/or requirements.

Standard Operating Procedure (SOP) Template

PURPOSE:

The purpose of this directive is to provide guidance to PSAP personnel in the event of a call for service that involves a social media post that may be of public safety interest that would require the dispatch of field responders.

POLICY:

This SOP is intended to implement policy on the use of the handling calls for service concerning social media posts by [AGENCY]. [NOTE: Insert/replace this text with your local agency's policy statement regarding adhere to SOPs]

PROCEDURES:

A. PSAP Authority for Use of Social Media Channels

Only staff authorized by the [POSITION, e.g., Communications Director] may use an existing [AGENCY] social media channel. This includes any social media channel (such as a particular [AGENCY] Facebook group or specific blog) that is managed by a [AGENCY]employee as part of their official duties.

Authorized staff shall respond to posts on social media channels as [AGENCY]. Personnel shall never use their personal social media accounts to respond to requests directed to [AGENCY]. Additionally, personnel shall never append a post on the agency's social media channel with his/her own name, badge number, or any other personal identity information.

B. Guidelines for Sensitive Information Obtained Over Social Media

A citizen may post sensitive medical or criminal information that is not considered public information. The Telecommunicator should make an effort to encourage the poster to call 9-1-1 directly or interact with the Telecommunicator via the platform's private messaging function, if available. If the citizen is not able or willing to establish contact directly, the Telecommunicator shall continue to triage the request for service accordingly.

Personnel shall never disclose any information via social media channels that is deemed confidential by law.

C. Guidelines for Handling Calls for Services Received over Social Media

PSAP personnel shall follow standard information gathering protocols for the receiving of and dispatching of calls for service including documenting any actions taken to process the call. Additional information should be gathered and documented that is specific to the social media post if available such as:

a. Social media site that the post was made on (e.g., Facebook, Twitter)
b. Screen name
c. The location of the posting on the social media site (e.g., individual's feed, group page, etc.
d. Any information on the user's social media profile (e.g., location, email address, or telephone number)
e. Any information that can be discerned from the social media provider (e.g., IP address, the geo-location of the post, if the user has location services enabled on their device)

It may be determined that the dispatchable location lies within another jurisdiction. This information should be provided to the responding agency for appropriate response.

PSAP personnel should attempt to record the social media post to document the incident in the event that the post is deleted. [AGENCY should provide some direction on how to accomplish this]

[AGENCY should provide policy and procedures for how social media sites are accessed from PSAP consoles]

D. Public Record Retention/Open Records

[AGENCY should consult their state laws governing the use of social media sites by a public agency and insert applicable language for record retention/Open Records in this section]

a) Agency Community Announcements
    a. Community announcements posted on AGENCY's social media accounts shall be managed by [INSERT APPROPRIATE AUTHORITY]. Personnel shall follow established guidelines for retention of public communications.
b) Calls for Service
    a. PSAP employees should not attempt to edit or delete posts on Agency social media accounts associated with calls for service.

b. PSAPs may want to document the source post of the call for service. Where possible, document:
   i. screenshot of the post including any agency responses
   ii. URL of the social media post
   iii. description of the post as provided by the poster, not paraphrased

ACKNOWLEDGEMENTS

The National Emergency Number Association (NENA) PSAP Operations Committee, Social Media Emergency Requests Working Group developed this document.

NENA Board of Directors Approval Date: 05/19/2022

NENA recognizes the following industry experts and their employers for their contributions to the development of this document.

Members	Employer
Pete Eggimann, ENP, PSAP Operations Committee Co-Chair	Eggimann Technology Services, LLC
Sandy Dyre, ENP, PSAP Operations Committee Co-Chair	DATAMARK
Lisa Dodson, ENP, Working Group Co-Chair	Motorola Solutions, Inc.
Andrea Wilson, Working Group Co-Chair	Montgomery County Emergency Communications District, TX
Brittney Burross	North Central Texas Council of Governments, TX
Adriana Cacciola	City of Chandler, AZ
Alex Graber, ENP	Waukesha County, WI
Ron Henri, ENP	Town of Cheshire, CT
Nick LaMontia, ENP	Kerr Emergency 9-1-1 Network, TX
Joseph Pennington, ENP	Chester County, PA
Scott Rose, ENP	Jefferson County Communications Center Authority, CO
Ann Treffer	University of Texas at Austin Police, TX
Koren Weer	Chester County, PA
Margaret Winter, ENP	City of Columbus, OH

Special Acknowledgements:

Delaine Arnold, ENP, Committee Resource Manager, has facilitated the production of this document through the prescribed approval process.

The NENA Social Media Requests for Service Working Group is part of the NENA Development Group that is led by:

- Wendi Rooney, ENP, and Jim Shepard, ENP, Development Steering Council Co-Chairs
- Brandon Abley, ENP, Technical Issues Director
- April Heinze, ENP, 9-1-1 & PSAP Operations Director