



Text Messages & Social Media in Public Safety

Public Records Policies & Best Practices

The popularity of SMS/text messaging and social media has exploded in recent years, both in our personal lives and in the workplace. Because of this, public safety agencies should be aware of certain guidelines and considerations when allowing employees to utilize these burgeoning communications tools. One such consideration is the role text messages and social media plays in open records requests, eDiscovery, and litigation events.

In this guide, we examine how public safety agencies can create policies that allow for compliant use of SMS/text messaging and social media, and how to retain and archive those communications for a more efficient response to open records requests.



Social media & SMS/text messaging amplify critical communications

For public safety agencies, the desire to use SMS/text messaging and social media to communicate across the department, with other agencies, and with the public, is on the rise largely due to an increasingly youthful, tech-savvy government workforce. Millennials make up the largest demographic in the government¹, and the impact this burgeoning generation has on workplace policies is already being felt.

More than 70 percent of adults in the United States now use social media platforms to connect with one another, engage with brands and news content, share information, and discuss what is happening in their community³. Meanwhile, the Smarsh 2018 Public Sector text & Mobile Communications Survey found⁴ that SMS/text messaging is the number one most requested communications channel among employees in the public safety sector, even beating out popular social media sites LinkedIn and Twitter.

The popularity of these new communications channels is undeniable, but the important question is this: What unique benefits can SMS/text messages and social media offer public safety agencies?

Let's look at SMS/Text messaging, the most rapid form of communication available. If you want to send crucial information and ensure it is read in a timely manner, you send a text message. According to the Pew Research Center, 98% of text messages are read within 2 minutes — a time savings that can literally mean the difference between life and death in an emergency.

PUBLIC SECTOR'S MOST REQUESTED² COMMUNICATIONS CHANNELS



42%
SMS/Text messaging



41%
LinkedIn



30%
Twitter

ACCORDING TO THE LATEST LAW ENFORCEMENT USE OF SOCIAL MEDIA SURVEY⁵, SOCIAL MEDIA PLATFORMS ARE USED FOR:

91% NOTIFYING THE PUBLIC OF SAFETY CONCERNS

89% COMMUNITY OUTREACH AND CITIZEN ENGAGEMENT

86% PUBLIC RELATIONS AND REPUTATION MANAGEMENT

Meanwhile, social media is a quick, easy, and effective way to communicate with citizens or groups. Social media can reduce the time it takes for first responders to get important information they need, such as emergency coordinates to help someone in danger. It can also help spread information rapidly to a wide swath of the community, which can be very useful in the event of public safety hazards or natural disasters.

But remember, any communication sent or received by government organizations — including public safety departments and their employees — is subject to open records requests.



A Community Outreach Officer with a western Massachusetts police department recognized the need to create more transparency and trust within the community he works for, based on the social media presence of the community he lives in. “I live in a different area than where I work. I saw how active my ‘civilian’ department was on social media, and it made me trust them even more as a member of the community. Their openness helped create a stronger sense of connection.” It was that connection the officer wanted to replicate on behalf of his police department.

“Of course, I use [social media] to alert the public about situations to avoid, such as road closures, construction, and accident scenes, but it’s so much more than that,” he pointed out. “Social media allows me to connect immediately. It also serves as an instant press release. I don’t have to wait for information to hit the wire and get picked up.”



Prohibition

A common reaction to employee requests to use SMS/text messaging and social media as approved means of communication has been blanket prohibition. In a perfect world prohibiting the use of a technology would be sufficient to avoid risk, but ours is not a perfect world. Like it or not, your employees are using SMS/text messaging and social media to communicate amongst themselves and with external contacts.

Even worse, ignoring or prohibiting the use of SMS/text messages can lead to risks including fines and increased litigation costs due to gaps in records management. All communications — including text messages and social media posts — must be considered public record if they contain work-related conversations or context, such as a message with photos from the scene of an emergency, or discussions between employees regarding incident response. When conversations happen without oversight or archiving, valuable records could be lost or deleted.

To comply with state, local, and federal laws such as the Freedom of Information Act (FOIA) and Sunshine laws, government organizations must be able to produce any business-related records requested by the public. If records cannot be produced quickly, accurately, and in their entirety, the organization may be subject to heavy fines, in addition to a damaged reputation and a lack of trust. The consequences of broken trust between public safety agencies and the communities they serve could pose negative challenges that put employees in danger when responding to an emergency or trying to build community support.








A policy of prohibition will not prevent employees from using social media and SMS/text messaging, but it will prevent your organization from supervising these communications channels.



Written policies

Whether SMS/text messages and social media are prohibited or not, departments should create and implement written policies. A solid policy includes clear rules of text messaging and social media interaction, and how those communications will be retained. These rules will help you meet public records requests — and permit your public safety employees to using mobile devices to communicate. Written policies should include:

- Who is permitted to use SMS/text messages and social media?
- What types of information can be sent using social media and SMS/text messages?
- An overview of the organizational device ownership scenario, including which carriers can be used.

	 Phones	 Tablets	 Laptops	 Apple iOS	 Android	 BlackBerry	 Windows
BYOD	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Government-issued	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- Which channels and applications will be allowed for devices?



Before finalizing your policy, get feedback from key stakeholder departments such as human resources, legal counsel, records-retention, and administrative departments who might have a role in determining the do’s and don’ts, and the consequences of non-compliance with your text message and social media policy. This creates top-down buy-in and makes sure the policies align with organizational needs and guidelines.

After the policy is finalized, you must train employees on the permitted use of SMS/text messaging and social media, and have them sign and date the policy. Review and update the policy on a regular basis, especially when new technologies are adopted into your communications strategies.

“The public wants information, and they want it instantly. The challenge for public safety agencies is balancing resources and accuracy against the need to produce instant information. Of course, regulations must be in place to assure first responders are not using social networking sites for personal reasons while on the job or out in the field. Social media and law enforcement can make a good team when used responsibly and proactively.”

– Jennifer Gavigan, Hadin Media Group

Personal social media accounts & professional conduct

An employee's personal social media pages and comments can be seen by the community as an extension of your organization and may reflect negatively on your agency. When it comes to personal social media pages, make sure your written policy:

- Provides rules for professional online conduct, including whether they are allowed to identify themselves as members of your department
- Clearly states if employees are required to provide you with access to their personal pages
- Outlines what types of content is off-limits, including certain types of videos, photos, third-party links, or commentary about hot-button topics

The benefits of a comprehensive archiving solution

As communications technologies evolve, it is important to be proactive in your approach to archiving conversations generated by your employees. Proactive archiving, where all relevant communications are automatically captured and stored in a search-ready repository, can make the difference between scrambling to find social media posts and text messages and being able to quickly locate records in response to an open records request. The alternative, which requires employees to store and submit their own communications data, is both a tremendous burden on IT and increases risk of missing or deleted information.

Instead, the best and most efficient way to manage and monitor social media posts and text messages — and ensure compliance with existing laws — is to have a comprehensive capture and retention system in place. To find a best-fit solution, take these features into consideration:

- **Automated process:** An automated system provides the secure capture of records with a minimal number of people involved to ensure the communications are properly retained and archived. This can also reduce the amount of time it takes to respond to a records request.
- **Robust search function:** Look for search functionality that not only allows you to perform basic searches but is also capable of handling wild-card and matching-word queries that will return all possible archived messages across all communications platforms. This enables you to produce the breadth of a conversation that may begin in one type of communication and concludes in another. This will also greatly reduce the time spent looking for records to satisfy requests.
- **Growth potential:** Think long term. Rather than investing in multiple standalone solutions for different content types that are limited in scope and may not work together as a unit, invest in a platform that will grow with your organization's needs and as new communication types (such as text messaging and social media) become available.
- **Direct-carrier capture:** A crucial feature of any archiving solution, direct-carrier capture allows you to pull communications data automatically from service providers, making ingestion easier, faster, and more effective.
- **What you see is what you get:** By law, records must be produced in their original context. Find a solution that not only retains social media and text message communications but keeps them in their original context and can show any deletions of the original record, who deleted it, and when. Also, avoid archiving systems that flatten communications into an email-like format, which negates the authenticity of the record.



The importance of authenticity

The authenticity of a record can be verified through its metadata, which is defined as data that provides information about other data. If an archiving system flattens records into an email-like format, the metadata is compromised.

Other ways to put metadata at risk include:

- Forwarding social media posts to an email address for retention purposes
- Taking screen shots of a post and sending the attachments
- Exporting social media posts and other content to an Excel file
- Photocopying text messages from a cell phone

If your employees rely on these methods, it's crucial that your organization immediately reviews and updates its organizational strategy on electronic communication records management. You'll likely also need to revise your user policies and train staff on allowed devices, applications, and communications.

1) <http://www.genfkd.org/more-millennials-in-government-than-before>

2) *Smarsh 2018 Electronic Communications Survey Report for the Public Sector*

3) <http://www.pewinternet.org/fact-sheet/social-media/>

4) <https://www.smarsh.com/whitepapers/2018-Government-Survey>

5) http://www.urban.org/sites/default/files/publication/88661/2016-law-enforcement-use-of-social-media-survey_5.pdf



Smarsh® delivers archiving solutions for the information-driven enterprise. Founded in 2001, Smarsh helps more than 20,000 organizations meet regulatory compliance, eDiscovery and record retention requirements. The company is headquartered in Portland, Ore. with offices in New York City, Boston, Los Angeles, and London.

