

Public Sector Guide to Text Messaging Policy and Retention



Capture and archive text messages confidently

This guide contains practical steps to help public sector organizations and departments develop a text message policy and retention strategy that will improve the efficiency of fulfilling public records requests while reducing the overall drain on resources. It also outlines some smart text recordkeeping practices, so you'll be better prepared to respond to open records requests or other e-discovery needs when they arise.



Are you capturing and archiving your text communications?

When you think of open records laws that apply to local and state, you might think email and official documents exchanged by officials are the only items that need to be archived.

However, text messages are considered a public record because in many instances they contain business conversations related to government work. When government employees are texting between mobile devices on the job, these messages are public records, and by law must be preserved.



Text messages ARE public records

The alarming thing is public sector organizations aren't giving text messages the same level of archiving attention as other forms of digital records. Many organizations don't have a solution in place for the retention and oversight of text messages, which causes problems and poses significant risk when facing an open records request, an investigation, e-discovery event, or litigation.

Texting and other types of digital communication are an essential tool for local governments, but they also present challenges that cannot be ignored. If you're concerned about your organization's ability to respond to text message records requests, there are proactive steps you can take now to avoid risk.

This guide will provide a few best practices to put policies, procedures, employee training, and records management technology in place to reduce text communications risk.

Carefully craft your text message policy



Even though text is easy, reliable, and intuitive — if it's used for official business communications, it can create tremendous risk absent an organizational use policy or archiving solution.

Collaboration across different departments in your organization is essential when building your text messaging policy, especially with your records management, IT, and legal teams. A sound organizational text messaging policy outlines which employees can use text for official business communications, and how that content will be retained — so you're prepared to meet public records requests, internal HR investigations, Freedom of Information Act requests, and conduct efficient e-discovery searches should litigation events occur.

Some key points to consider when developing your text messaging policy, procedures, and employee training:

How do your employees plan to use text messaging?

Understanding the intent of your employees' use of text messaging is important. You may find they want to use it to:

- ✓ Maintain business relationships and cross-departmental communication within the organization
- ✓ Connect with government vendors and partners on an ad-hoc basis
- ✓ Increase the reach of standard emergency communication methods
- ✓ Connect with colleagues or influencers at other public sector agencies

High-level Michigan State Police officials were charged in 2021 for **downloading an app that deletes text messages on their state-issued cell phones**. This is a direct violation of the state's Freedom of Information Act.¹

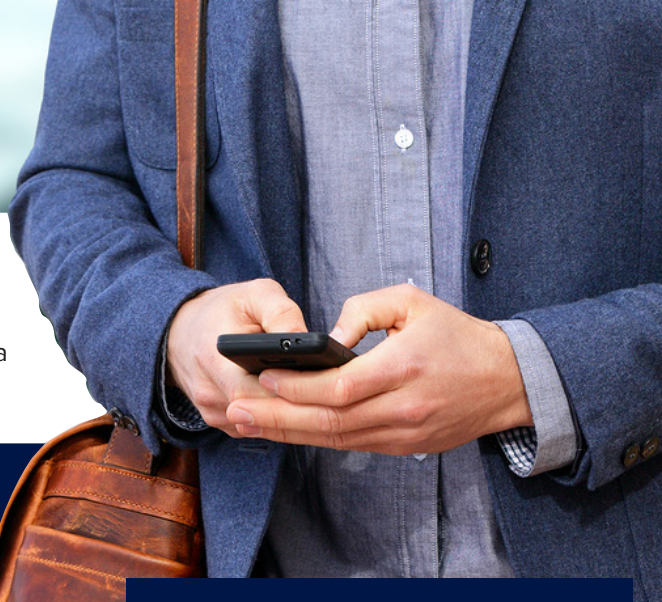
What devices do your employees already use for text messaging? Which devices will you allow?

It doesn't matter if an employee uses a government-issued device, a personally-owned device, or a combination of the two for business-related texts. All are fair game for public records requests and discovery in litigation if they contain relevant, official government communications.

Keeping this in mind, your organization may wish to create a policy that states employees may only use government-issued devices for business text communications. Or, your organization may allow business text communications and employee-owned personal devices. Whichever you choose, employees must be made aware that text communications on either type of device are business records and require ongoing monitoring and archiving. Consequences for failure to follow policy should also be stated.

Note: It's important to specify if employees may use government-issued devices for personal text messages (for instance, to a family member), and if so, whether those messages will be subject to archiving.

¹<https://www.freep.com/story/news/local/michigan/2021/01/22/state-police-phone-apps-keep-text-messages-secret/4236305001/>



Who's doing the texting?

Your text messaging policy should identify which employees are authorized to use text messaging for business communications. Or will you only allow a select group of individuals to use it?

67% of organizations face major risk for fines and litigation in the absence of a sound SMS/text capture strategy

What are your state's legal requirements?

Start by reviewing and documenting the legal requirements, open records laws, guidelines, and regulations related to text messaging that your organization is required to follow. In addition, determine your organization's required records retention periods.

Detail every requirement regarding records retention laws and regulations. Collaborate with legal counsel, human resources, compliance, the records-retention officer, records clerk, or other departments to specify the "do's and don'ts" and consequences of non-compliance with text messaging procedures.

How will you train employees on proper procedures for text messaging? Who will train them about what can and can't be communicated via text messages? Training should explicitly educate employees about the difference between official business communication and personal/transitory communication. If your employees use text messaging in a personal capacity, the policy should detail rules and procedures for conduct on personal and official devices.

iMessage should be disabled on iPhones used for business texts because those messages cannot be archived.

Apple has a Device Enrollment Program (DEP) available that can help public sector organizations easily deploy and manage government-issued iOS and OS X devices — and enable control over iMessage so it can be shut off. Many public sector organizations may then use a Mobile Device Management (MDM) solution in conjunction with Apple's DEP to automate provisioning of devices and manage and supervise their functions.

The ideal solutions provider will work directly with carriers including:



AT&T



CellTrust



RingCentral



T-Mobile



US Cellular



Verizon




Zoom

If your agency's employees use text messaging for business communication, they need to know messages will be archived in line with state open records laws, Freedom of Information Act requirements, and e-discovery and legal obligations.



The Seattle Times filed a lawsuit in 2021 alleging that the city of Seattle **mishandled requests from reporters for officials' text messages**. The complaint follows a whistleblower investigation that found the Seattle Mayor's Office violated state public records laws in its handling of requests after discovering the mayor's texts were missing for a 10-month period.²



Which employees need to read, review, and sign the text messaging policy? Have a system in place to distribute your text messaging policy to employees, with specific actions outlined for individuals who need to sign and acknowledge the policy.

Once you have developed a policy, it's time to review how your organization retains text messages. To comply with many state recordkeeping standards, you will need to update your archiving practices and technology if you find employees are:

- ✓ Taking screen shots of text messages to create records
- ✓ Forwarding text messages to email to retain them
- ✓ Relying on wireless carriers to keep the records
- ✓ Exporting their text messages to Excel files

To support records compliance, text messages must be properly archived and producible. To ensure the authenticity of the record, the associated metadata must be captured. It is important to note that producing electronic records using any of the methods listed above removes the authenticity of the communication — which may leave you vulnerable during litigation.

When your policy is complete, you'll have documentation that allows your organization to confidently communicate via text messaging.

Using precise language will help your organization operate within the boundaries of various government records requirements and allow you to respond to any request for text messaging records during an investigation, e-discovery, or litigation event. Remember to review your text messaging policy over time to keep up with the needs of your organization, changing technologies, and new regulations.

² <https://www.seattletimes.com/seattle-news/seattle-times-sues-city-of-seattle-over-missing-durkan-text-messages/>

Smart text message capture and archiving for the modern government

Technology and automation should make life easier for your organization. Safe, secure, and automated capture of text message records is the goal. Proactive archiving can make the difference between a records or legal team that's burdened by antiquated processes to manage text messaging and related requests, and one that supports it because they have an effective way to manage, monitor, and produce text content.

A smart archive includes:

Smart ingestion – real-time capture

This eliminates the possibility of employee text messaging data being deleted. If an employee texts someone but later deletes it, you'll see the original text message in the archive, plus an activity log that shows who deleted the text, and when it was deleted.

Thorough, efficient search

Your department should be able to run searches on their own and get results back within seconds, without the need to seek assistance from IT or your archiving vendor. If you choose a solution to index text messages along with other allowed content types such as instant messaging, collaboration, and social media — records teams will be able to review fully threaded conversations to see the context of messages, updates, and comments in one consolidated destination.

Universal search and production

You don't need to have multiple archiving vendors for individual content types, such as email, text, and social media. A better option is to use a single comprehensive archiving solution that archives all content types. This allows you to simultaneously and quickly search across people, keywords, and content types to return universal results, with no stone left unturned.

Automation through policy management

Smart policies that scan content from your organization's text messaging accounts for specific information as the data enters the archive can help your legal and records team become ultra efficient and more diligent with discovery and production. Policies can help you automate more manual processes, such as your retention schedule.

On-demand access

Producing text messages quickly in response to records requests is mission critical for government organizations. Your archive must include text messages regardless of the mobile operating system, carrier, or device. Whether your organization issues the mobile device, allows employees to use their own personal device, or supports a combination of the two, make sure your archiving solution is flexible enough to meet your needs.

Local governments benefit from a public records portal

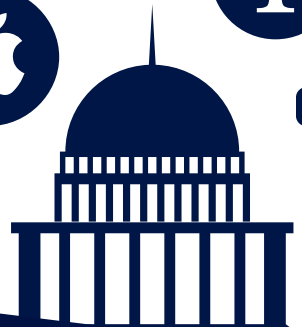
Producing content to fulfill public records requests is crucial, but a process that starts with a straightforward, intuitive public records portal that allows journalists and constituents to submit requests and ends with prompt delivery is key.

Smarsh and NextRequest have partnered to simplify the process of responding to public records requests by providing a robust end-to-end solution, the first of its kind for state and local governments.

NextRequest provides an online portal for constituents and journalists to submit public records requests, as well as a platform for government agencies to efficiently manage and respond to these requests. With this integration, electronic messages that are captured and archived by these entities can be integrated efficiently into the record request workflow.

Meanwhile, Smarsh offers automated and secure capture, retention, and review of digital communications. Digital records are ingested and stored in their native format, and available in an easily searchable format (across all communications channels).

Larger public sector organization can also choose a Smarsh on-premise text message archiving solution, which enables full control of text archiving within the organization's own servers or their own cloud account.



Smarsh enables companies to transform oversight into foresight by surfacing business-critical signals in more than 80 digital communications channels. Regulated organizations of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisors and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com.

Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions. You must consult your attorney regarding your compliance with applicable laws and regulations.

