

The Public Sector Guide **to Text Messaging Policy and Retention** 2017 Edition

Use text messages for business communications with confidence.

This guide contains practical steps that will help public sector organizations and departments develop a text message policy and retention strategy to protect against the risk involved with use of this popular, universal form of communication. 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.

smarsh®





What's the Big Deal About Text Messages?

When you think of open records laws that apply to local, state, and federal government, 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. Sending text messages between mobile devices is now public business, and by law, the records need to be preserved.

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.

If you're concerned about how your open records practices are keeping up, and are scrambling to accurately identify risk within your organization, there are proactive steps you can take now. Texting and other types of electronic communication are a valuable tool for local governments, but they also present challenges that cannot be ignored any longer.

Right now, it's best practice to put policies, procedures, employee training, and archiving technology in place to reduce text communications risk.

Carefully Craft Your Text Message Policy



Texting is simple, concise, and compatible with virtually every mobile device, operating system, and wireless carrier—making it extremely accessible when a government employee wants to communicate in a time-crunched world. But even though text is easy, reliable, and intuitive—if it's used for official business communications, it can create tremendous risk.

A solid policy includes clear documentation that outlines the rules of text messaging interaction within the organization, and how that content will be retained—so you're prepared to meet public records requests, Freedom of Information Act requests, and e-discovery and litigation events.

Collaboration across different departments in your organization is ideal when building your text messaging policy, especially with your records management and legal teams.

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



Why do your employees want 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

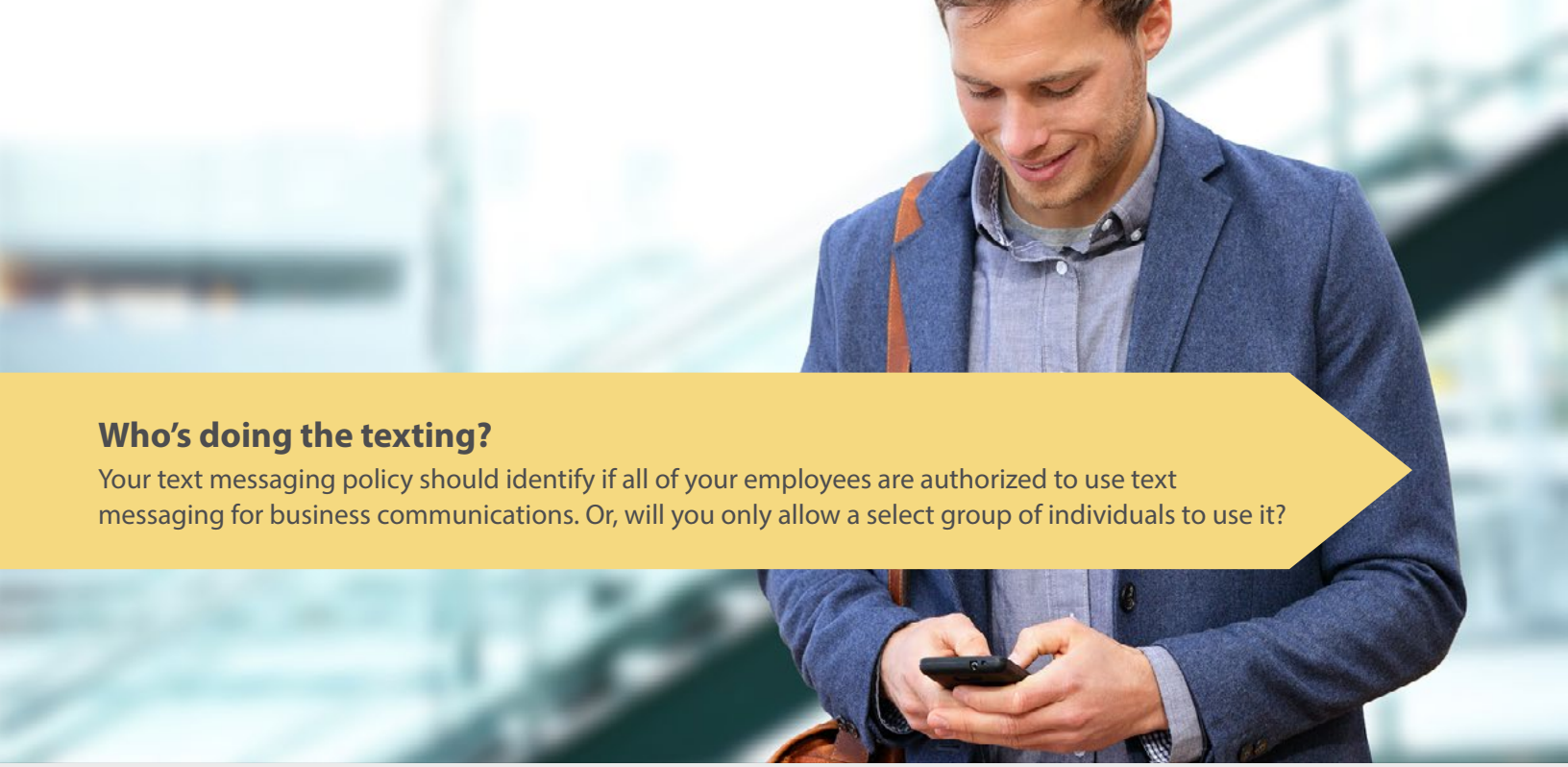
What devices do your employees already use for text messaging? Which ones will you allow?



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 text communication on government-issued devices 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.

You may also want to specify if employees are allowed to use government-issued devices for personal text messages (for instance, to a family member), and if so, whether those messages will be subject to monitoring and archiving.



Who's doing the texting?

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

Do you know all your regulatory and legal requirements? Is your organization fully aware of all the legal requirements, open records laws, guidelines, and regulations related to text messaging that your organization is required to follow? In addition, do you know your organization's required records retention periods? If you'd like to check out your state's open records laws, see the Reporter's Committee Open Government Guide.

Detail every requirement regarding records retention laws and regulations. Pull in 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.

Tell employees that text messages related to official business communications will be made available for archiving. 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.

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.

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 technology, and new regulations.

Once you have developed the policy, it's time to review how your organization is 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.

Smart Archiving for Smart Government



Technology and automation should make life easier for your organization. Safe, secure, and automated capture of text messaging records is the goal. Proactive archiving can make the difference between a records or legal team that's stressed by text messaging, 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.

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

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.

The Archiving Platform™ from Smarsh is a leading, cloud-based, comprehensive archive platform supporting a broad range of content types, including email, instant and text messages, web, video and text messaging. Core features include immutable retention of all archived content in an indexed and search-ready state, policies, cases and admin/reporting functions. Core features can be extended and enhanced with specialized workflow add-on modules for message supervision/review, discovery, and personal access to archived email from any device, including mobile ones.

In addition, Smarsh now offers a hosted text message archiving platform for federal, state, and local customers using Amazon Web Services GovCloud.

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



WHY SMARSH?

Smarsh® delivers cloud-based archiving, search and analytics solutions for the information-driven enterprise. Its platform enables organizations to archive, search, supervise and produce the entire range of digital communications from one central location, including email, public and enterprise social media, Web, instant messaging and mobile messaging.

Founded in 2001, Smarsh helps more than 20,000 organizations meet regulatory compliance, e-discovery and record retention requirements. The company is headquartered in Portland, Ore. with offices in New York City, Boston, Los Angeles, and London.

1-866-762-7741 | **www.smarsh.com** @SmarshInc SmarshInc Companies/Smarsh

© Copyright 2017 Smarsh, Inc. All rights reserved.