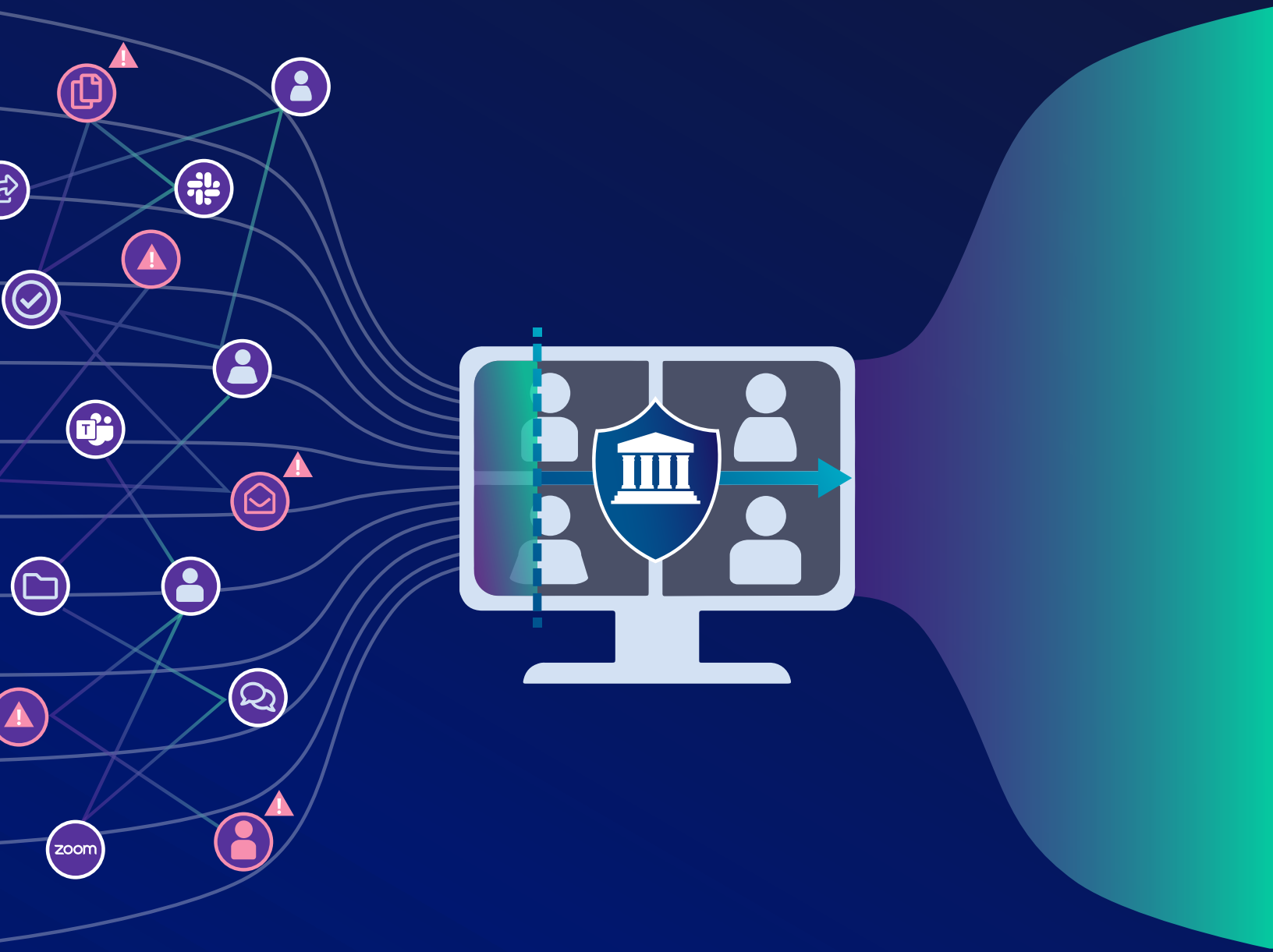
smarsh®

Risk Management Policies for Government Text Messaging, Email and Social Media



Government employees today use a combination of communications tools and devices to perform their jobs. And the need for a wider variety of communication channels has only grown more imminent. The prevalence of remote work due to the pandemic increased our reliance on mobile devices and a multitude of applications to stay connected.

The Freedom of Information Act (FOIA) and state sunshine laws require public agencies to preserve and produce communication records. These records can be pertinent to legal discovery and internal investigations, making it even more critical to proactively collect and preserve them.

Public-facing communications like social media and the use of mobile texting and multiple email accounts are creating growing volumes of public records that government agencies have to manage. Responding to public records requests and investigations has become unwieldy—consuming time, staff and financial resources. In today's world of instant communication, the public expects immediate responses and more efficient government spending.

Staying ahead of records requests requires a thorough understanding of the tools your organization uses to communicate and how you manage the content generated through each platform. Ensuring an efficient process and comprehensive compliance with open records laws requires:

- Understanding the unique risk factors of each communication channel
- Implementing usage policies for government employees
- Adopting modern archiving technology to securely collect and preserve cross-platform communications

In this guide, we highlight common risk factors associated with text messaging, social media and email, and recommendations to help you mitigate risk and strengthen your public records program.

First steps to minimizing risk

1. **Know your state's requirements.** Nearly every state has documented public records retention policies for electronic communications. Make sure you are familiar with your state's policies for public records and the record retention schedule (how long you need to keep records). For quick reference, check out the Smarsh Interactive Map of Sunshine Laws by State for definitions and outlines of records, meetings and litigation disclosures.

2. **Assess and update your technology.** Citizens' ability to access public records is a necessary instrument of a transparent government and informed constituency. In today's reality, where people communicate across multiple applications and devices, managing the volume and variety of these records can be overwhelming. Agencies can replace inefficient, paper-based and manual processes with comprehensive, easy-to-use archiving technology. This enables them to find and produce the information they need more easily to reduce overhead costs.

3. **Develop use policies and train your staff.** This is what we'll cover in this guide. It's critical to provide your employees with acceptable use policies, including explicit guidelines around which applications and devices are allowed or prohibited.

TEXT MESSAGING

Texting has become a go-to channel for people to communicate—both personally and on the job. As the pandemic moved many people to remote work, studies have shown that mobile device usage during typical working hours has increased.[1] Text messaging is a convenient way for workers to connect quickly on important subjects. For example, in law enforcement, a quick response to a text message can be critical during an emergency.

RISK FACTOR

Mobile carriers don't save text messages

A pervasive myth in the public records world is that mobile carriers save text messages. However, these providers don't have any legal responsibility to keep or retrieve their customers' text message content. Here are the policies for some of the major companies (as of April 2020):

- **Verizon:** Customers can only retrieve text message content that was sent or received within five days of the request
- **AT&T:** No records are kept of customers' text messages
- **Sprint:** No message content is kept. Customers may access message data, but that would only include the time, date and phone numbers involved with the text
- **T-Mobile:** No message content is kept. Customers may access message data, but that would only include the time, date and phone numbers involved with the text

If agencies can't rely on mobile providers, they're likely performing laborious, error-prone forensics like screenshotting or photocopying text messages. This isn't a scalable or sustainable solution.

Policy recommendation:

While some agencies implement an organization-wide policy advising against the use of texting, it only takes one errant text to put the agency at risk. Instead of trying to prevent text messaging at work, public agencies can minimize risk and ensure compliance with recordkeeping rules with adequate usage policies and tools to capture and retain all text messages.

Technology recommendation:

If your agency allows staff to use their personal devices to communicate, we recommend you check out our BYOD Checklist: Managing Personal Devices in Government. In it, we cover the benefits of working with an archiving provider that has established direct partnerships with popular mobile carriers for content capture.

A county was sued for omitting text messages in a public records request. One of the officials listed in the lawsuit argued that he fully complied with the request as quickly as possible, but was delayed by his cell phone provider, which provided incomplete logs of text messages.[2]

1 https://www.businesswire.com/news/home/20200505005144/en/Valassis-Real-time-Insights-Inform-Marketing-Strategies-COVID-19
2 https://www.bradenton.com/news/local/article248052940.html

EMAIL

Though it's seen increasing competition from social media, text messages and collaboration platforms in recent years, email remains the go-to channel when it comes to official business communication.

> The total number of business and consumer emails sent and received per day is forecast to grow to more than 347 billion by the end of 2023.[3]

RISK FACTOR — Personal email accounts

Personal emails are typically not being archived. Messages can easily be deleted and hard to recover, making it difficult for staff to fulfill public records requests when those emails are used to conduct government business.

Policy recommendation:

The safest way to avoid having to retrieve emails from personal accounts is to prohibit employees from using their personal email accounts for any government-related business. However, if emails relate to staff, vendors or organizations that are tied to government, they are public record. When creating an email policy, we recommend you document explicit rules about the use or prohibition of personal email addresses for work-related matters and create an Employee Acceptable Use Agreement for signed acknowledgement of policies.

Technology recommendation:

Many government organizations archive their email on premise—which requires IT to search and produce email data each time a request is made. Modernization is crucial if your organization hopes to respond in timely fashion to records requests while freeing up time for your IT team. Not to mention, a cloud-based archive is a single source of truth; rather than performing inconvenient forensics practices for single emails, the ability to search for multiple records within one secure database makes the process quicker and reduces the chances of error.

> **Remember:** if it can't be archived, it shouldn't be used for work-related matters.

3 https://www.lifewire.com/how-many-emails-are-sent-every-day-1171210

SOCIAL MEDIA

Social media is a useful tool for community engagement. It provides a platform to relay critical information to the public and hear concerns from members of the community. Social media offers a face to government, which can strengthen trust between the agency and the community it serves.

RISK FACTOR	Trolls (disgruntled commenters)

Policy recommendation:

A solid social media policy includes clear rules of social media interaction, and how those communications will be monitored and retained. These rules will help meet public records requirements and provide guardrails for public employees to communicate on social channels. Written policies should describe:

- Who is permitted to administer the agency's social media accounts
- Rules for employees using personal accounts to discuss government business (if this is allowed, how will that content be preserved?)
- What types of information can be shared, and rules for comments and responses on social media
- Consequences of noncompliance with social media policy

After the policy is finalized, employees need to be trained on the permitted use of social media. Review and update the policy on a regular basis, especially when new technologies are adopted into the agency's communications strategies.

DON'T FEED THE TROLLS

1. Do not delete these comments. You may choose to hide them but allowing them to be preserved and monitored ensures evidence in case of legal issues
2. Acknowledge their complaint so they know they've been heard
3. Have empathy—whether it's a bot or an angry constituent, be a good example
4. Know when to move the conversation offline or stop responding

Technology recommendation:

An archiving solution that collects and preserves all social media communications and activity can be used as the first line of defense against malicious commenting and potential legal action. Make sure your archive can preserve contextual details:

- The original post and all related comments and reaction activities
- Revisions and/or deletions of posts and comments
- Time and date of posts and other associated metadata

ARCHIVING COMMUNICATIONS TO SAVE TIME AND RESOURCES

As communications technologies evolve, it is important to be proactive in archiving conversations generated by employees. Proactive archiving, where all relevant communications are automatically captured and stored in a search-ready repository, makes all the difference when responding 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 the risk of missing or deleted information. 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 processes

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 capabilities (by name, keywords or content channel) that will return all possible archived messages across all communications platforms. This allows for easy retrieval 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 the agency's needs and as new communication types (such as text messaging and social media) become available.

Data integrity and security

By law, records must be produced in their original context. Find a solution that not only retains social media, email and text message communications but keeps them in their original context with secure controls that prevent records from being altered or tampered with once collected. The solution should have the capability to identify 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.

HOW SMARSH CAN HELP

Smarsh enables state and local government agencies to respond to public records requests quickly and thoroughly. Smarsh archiving solutions support over 80 different communications channels across email, SMS/text, social media, IM/collaboration, voice and web. Smarsh simplifies text message archival by partnering with carriers like Verizon, AT&T and T-Mobile. These partnerships allow Smarsh to seamlessly capture and retain text message content directly from the carriers.

Smarsh solutions help government agencies:

- Modernize records management and production
- Automate forms and hard-copy handling
- Free IT from continuous search and triage of information
- Reduce risk of fines from delays or incomplete information
- Build public trust and transparency

As communication habits continue to evolve with emerging technologies, it's not efficient or effective for agencies to continue playing catch-up with their policies. Government agencies need to better position themselves to meet information governance objectives in the digital age. With the right blend of archiving technology and internal policies, governments can reduce the risk of fines and legal issues as they modernize their approach to records management.

smarsh®

Smarsh® is the recognized global leader in electronic communications archiving solutions for regulated organizations. The Smarsh Connected Suite provides innovative capture, archiving, e-discovery, and supervision solutions across the industry's widest breadth of communication channels.

Scalable for organizations of all sizes, the Smarsh platform provides customers with compliance built on confidence. It enables them to strategically future-proof as new communication channels are adopted, and to realize more insight and value from the data in their archive. Customers strengthen their compliance and e-discovery initiatives, and benefit from the productive use of email, social media, mobile/text messaging, instant messaging and collaboration, web, and voice channels.

Smarsh serves a global client base that spans the top banks in North America and Europe, along with leading brokerage firms, insurers, and registered investment advisors. Smarsh also enables federal and state government agencies to meet their public records and e-discovery requirements. For more information, visit www.smarsh.com.

US: 1-866-762-7741 | UK: +44 (0) 20 3608 1209 www.smarsh.com @SmarshInc SmarshInc Company/Smarsh