Ohio Electronic Records Committee
Tip Sheet

Tips for Text Messaging Retention

Text Messaging Defined:

Text messages, communications received and sent via a mobile device like a cell phone, may be a government record. Like paper or email, text messages are just another format on which information can be affixed. If that information concerns the work of your public office (ORC 149.011), then it is most likely a record of the office to be retained per your official records retention schedules. Regardless of whether the device is owned by the office or is the individual's personal device, text messages meeting the definition of a record are a record of your office.

Is Your Text A Record to be Retained Per Retention Schedule:

- Does it document a business activity, transaction or decision?
- Is it proof of a business-related event or activity or evidence of work completed?
- Do you need it to identify who participated in a business activity or had knowledge of an event?
- Does it have legal or compliance value?
- Could it help resolve a dispute in the future?
- Does the law expect that the office will retain it?
- Do you have the only copy within the office? (ex. It was received from an external source)
- Are you the author responsible for managing it and its responses?
- If it were in paper form, would it be retained?

Risks and Liabilities to Using Text Messages for Government Business:

Text messages used for business purposes prove challenging to maintain as a record of the office.

Illegal destruction of records - $1000 per message (ORC 149.351)

Unable to provide prompt responses to public records requests – violation of public records laws (ORC 149.43)

Discovery and Litigation Costs

Basic capture technology does not preserve metadata

Reputational exposure

Making copies of everything on a phone increases the time and resources needed to locate and preserve pertinent messages and cannot account for deleted messages.

Retaining messages beyond stated retention would require more time and resources to locate and compile under public records and/or discovery requests.

Inadvertent information exposure

Potential violation of Open Meetings Law (ORC 121.22)

Best Practices to Try:

1. **Policies & User Agreements** – As employees are hired, they should sign off on an acknowledgement that they understand that text messages and mobile devices may be or contain records of the office even on their own devices. The policy should also clearly state that mobile devices may be collected or reviewed for public records or litigation purposes.
2. **Technical Solutions/Controls** – Vendors offer software products and services which can capture, tag, archive, or backup messages as they are sent and received. These are not one-size-fit-all solutions, but can provide a means to collect messages needed for a public records request or in discovery review and can be setup with oversight from your IT services.
3. **Asset Inventory** – "Office-Issued" mobile devices should be included in an organization's asset inventory. This will allow IT services to know which devices would need specialized applications added or updated, which then could be backed up, and upon employee separation, should be collected. It may also be beneficial to note those personal devices being used if your office allows "BYOD".
4. **Buy-In** – The successful implementation of a text messaging management plan is dependent upon buy-in and participation from several areas of your office: Legal counsel, IT, security, records management, Records Commission, etc.

Pros and Cons to "Office-Issued" and "BYOD" Phones:

If the choice is made to allow text messaging, agencies can either provide government-issued devices or allow a "bring your own device" (BYOD) policy. Below are some considerations for each approach:

***Office-Issued Phones* Approach**

PROS	CONS
Ability to install controls software	Employees may use phones for personal use
Asset tag and track device	Costs – device, service fees, data storage
Texts of separated employees retained	Employees would carry 2 phones
Ability to retain despite end-user actions taken (ex. Deletions)	

***Bring Your Own Device (BYOD)* Approach**

PROS	CONS
Reduces organization technology costs	Business records intermixed with personal
Staff prefer not to carry two phones	Increased legal costs and liability
Organization benefits from users' desire for newer technology	More difficult to obtain for public records & litigation
	Difficult to enforce retention & disposition requirements
	Employee(s) take public records with them when they separate
	Employee(s) could lose access to their phone if attorneys need to get information from it
	Data security risks
	Lack of end-user support from the organization
	Increased costs for mobile management software

OhioERC
Ohio Electronic Records Committee