CoSA
Council of State Archivists

DOCUMENTING GOVERNMENT
PROMOTING HISTORY
SECURING RIGHTS

Managing Electronic Communications in Government

www.statearchivists.org

Email, text, instant messages, and social media have changed the way government agencies communicate with their employees and the public, but records management concerns are often neglected. Consider these points to help keep your agency out of legal trouble and ensure that critical records are preserved.

- **Content, not format, is important.** Just as you wouldn't keep a letter on yellow paper longer than one on white paper because of its color, you wouldn't keep or destroy communication based solely on format. Whether a message is sent via email, text, social media, or other means, the content of the message is what determines its value and retention.
- **If public business is being conducted, it's a government record.** Not all communications rise to the level of official record, but generally if you're conducting official government business any related communication is a record. Check with your state or local authorities for your specific legal and retention requirements.
- **Public business on private accounts is still public.** As recent news stories and court cases have shown, private accounts and personal devices are subject to public records laws if they are used to conduct public business. This helps ensure transparency in government and accountability of public employees and officeholders.
- **Avoid combining public and private communications.** In the event of a FOIA, sunshine law, public records, or e-discovery request, your correspondence may be searched. Keep personal and business communications separate if you wish to protect your privacy.
- **Understand third-party tools.** Using social media or text messages for government communication complicates the process of capturing and preserving records, since these platforms are typically operated by parties outside of government. Agencies must clearly understand the limits and user agreements of the technologies being used and plan for records management *before* information requests come in.
- **Bring Your Own Device (BYOD) considerations.** Both records management and information security can be a challenge when allowing employees to use their own devices for public work. Clear policies regarding the use of such devices are essential, as are plans for retrieval of record information from those devices. Mobile Device Management software can help, but only if implemented properly.
- **Is there a policy for that?** Government agencies should have policies in place that clearly explain how each communication technology should be used, set limits on what content may be transmitted by such technologies, and outline procedures for retention, retrieval, preservation, and disposition of communication content. Both record and non-record communication should be addressed.