ADMINISTRATIVE PROCEDURE

SECTION:600 – Information Technology	**PROCEDURE #: 601-A**
TITLE: Texting	**IMPLEMENTS POLICY #: 601**
SPONSORING DEPARTMENT/DIV: Department of Information Technology Services (ITS)	
EFFECTIVE DATE: 10/18/2016	**REVIEWED: 2/12/2026**

OBJECTIVE: To establish procedures for protecting and maintaining the County's public records and other information from the risks created by text messaging.

PROCEDURES:

1. Risks of Texting.

   The County is legally required to maintain public records and to safeguard restricted and confidential information. Transmitting information via wireless text messaging using carrier-supplied standard applications poses several risks, including:

   1.1. Text messages are not encrypted.

   1.2. Text messages can be forwarded, shared, or stored by recipients.

   1.3. Unintended recipients may receive text messages.

   1.4. Text messages may be used as evidence in legal proceedings.

   1.5. Text messages relating to County business are public records that must be maintained, but are not stored on the County network. There is no centralized system for archiving text messages subject to Public Records retention requirements. Therefore, workforce members using text messaging assume the responsibility of assuring the content is retained.

2. Acceptable Use.

   2.1. Workforce members must use the County-managed secure texting application.

      2.1.1. The County-managed secure texting application is not approved for HIPAA-related content.

2.2. Workforce members must obtain approval from their supervisor to use texting in the conduct of County business. The approval should specify the types of situations in which texting will be used as a communication tool.

2.3. Workforce members are responsible for ensuring recipient phone numbers are accurate and periodically contacting text message recipients to determine whether they want to continue to communicate via text messaging.

2.4. As a best practice, workforce members should avoid sending or receiving text messages that:

2.4.1. Include information identified as "Restricted Data" or "Confidential Data".

2.5. Workforce members who are contemplating the risks of text messaging and find it necessary for their job to use this communication method must collaborate with their designated Public Records Officer. This collaboration is essential to ensure that their text messaging practices comply with retention requirements.

3. Guidelines for Public Records Retention - Managing and Retaining Public Records Stored on Mobile Devices.

3.1. Text and Instant Messages.

3.1.1. Text messages sent and received while conducting County business must be retained in accordance with Public Records retention rules. Only mobile devices intentionally used for generating and receiving texts relating to County business, requiring either retention or secure processing, are to be enrolled in the County's secure texting service.

This service provides an application that secures messages during transmission, limits the lifespan of messages on the mobile device, and offers an automatic, secure retention service on a hosted server.

See Procedure 601-B for guidance on Instant Messages.

The County-managed secure texting application will retain all messages for 10 years. Workforce members are obligated to move all text messages to longer-term solutions when the 10-year threshold is insufficient to fulfill the retention requirement for a text message due to its content.

4. Responding to Messages Requiring Retention and Security Received Through Carrier-Provided Text Messaging Services.

4.1. Even if a Workforce Member tries to avoid sending or receiving messages that must be kept under retention rules, it's still possible to get such messages through regular texting applications. When that happens, the Workforce member remains responsible for ensuring that those messages are handled properly. To meet retention and security requirements, the following options are:

- **Option 1: Text-to-Text For Non-Confidential Information Subject to Retention**: If you receive a message that must be retained according to Public Record requirements but is not Confidential, you must forward it from the source texting application to the County-managed texting application. Important: Do not send Confidential information via text. If the message is Confidential, follow Option 4 instead.

- **Option 2: Text-to-Text For Confidential Information Subject to Retention:** Copy/Paste information from the source testing application into the County-managed secure texting application, and then it can be sent to appropriate personnel.

- **Option 3 – Email the Message (For Non-Confidential Information Subject to Retention)**: If the message must be retained but is not Confidential, you can copy the text and paste it into an email addressed to your County email account. Send the email and keep it in your email archive in accordance with the County's retention rules. The email will automatically include the date, time, and recipient of the message.

Important: Do not email Confidential information —use Option 4 instead.

- **Option 4: Manual Transcription (For Confidential Information):** If you receive sensitive information through regular texting, do not forward or email it. Instead, write down (or transcribe) the message, including the date, time, and sender's name. Keep the transcription in a secure location and retain it in accordance with Public Records rules.

This is the only safe way to keep Confidential messages received outside the County-managed secure texting application.

4.2. Documents, Photographs, Audio Files, and Video Files

If you create or receive any files on your mobile device that constitute Public Records (e.g., documents, photos, audio files, or video files), send them as email attachments to your County email account. Then, keep them in accordance with the applicable Public Records retention rules.

If the file is too large to email, contact the ITS Service Desk for help.

5. Guidelines for Safeguarding Text Messages Containing Confidential Data.

Workforce members should take precautionary measures to ensure that their device is safeguarded against theft or unauthorized access to stored data. This includes but is not limited to:

5.1. Ensure the mobile device is enrolled in the County-managed secure texting application.

5.2. Ensure the device is password-protected and is configured to time out after no more than 15 minutes of inactivity.

5.3. Delete messages at the earliest opportunity.

5.4. Report theft/loss of a device as soon as possible. To report the loss of a device or any security concern, please submit an Incident and Risk Assessment Form during business hours and contact the ITS Service Desk. If it is after hours, also contact the Sheriff's Office Records Division.