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: 07/01/2024**

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

APPLICABILITY:

This policy applies to:

1. All workforce members engaged by the County to use information technology in support of County business. This includes but is not limited to employees, contractors, consultants, temporaries, volunteers, and interns.
2. All information technology owned and controlled by the County as defined below.

DEFINITIONS:

1. Technology Owned and Controlled by the County:
    a. All electronic information and communications created, processed, or stored on networks and devices owned and controlled by the County.
    b. All electronic information and communications relating to County business regardless of where the records are stored, including but not limited to, on personally owned devices, portable mass storage media, the "cloud" or externally provided services and personal email services.
2. Protected Information: Includes confidential, sensitive, and/or information that is protected under the law or County Policy.

PROCEDURES:

1. Risks of Texting.

   The County is legally required to maintain public records and to protect confidential, sensitive and protected information. Transmitting information by wireless text messaging, utilizing carrier supplied standard applications, poses several risks, including:

   1.1. Text messages are not encrypted.

   1.2. Text messages can be circulated by recipients or forwarded and may be stored.

   1.3. Text messages can be received by unintended recipients.

   1.4. Text message senders can misdirect text messages.

   1.5. Text messages can be used as evidence in legal proceedings.

   1.6. Text messages are public records that must be maintained but are not stored on the County network.

   1.7. There is no centralized system for all archiving text messages subject to Public Records retention requirements. Workforce Members using text messaging assume the responsibility of assuring the content is retained.

2. Acceptable Use.

   2.1. Workforce Members must use an ITS approved secure text messaging solution.

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

   2.3. Workforce Members are responsible for ensuring recipient phone numbers are accurate and to periodically contact text message recipients to determine if 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. Are subject to public retention laws; and/or

2.4.2. Include protected information.

2.4.3. Include information identified as “Confidential”.

2.5. Workforce Members considering the risks associated with text messaging who determine it prudent or job essential to utilize text messaging, are obligated to work with their Department designated Public Records Officer to validate that their process aligns 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 approved secure texting service.

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

3.2. The County standard text messaging application will provide 10 years of retention for all messages. Workforce Members are obligated to move all text messages to longer term Outlook retention folders when that 10-year threshold is insufficient for fulfilling the retention requirement for a text message due to content.

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

4.1. It is recognized that despite the Workforce Member’s intentions to avoid generating and receiving messages subject to retention policies, it is not possible to prevent the receipt of messages containing such content from senders through the standard carrier provided text messaging client outside of the secure text messaging service. The Workforce Member’s obligations extend to assuring that retention and security requirements are addressed. The following options to assure appropriate retention are outlined.

- Option 1 – (When the information received requires retention, but retention is not sensitive.) Text-to-Text. Forward the text messaging from the standard client to the County provided secure text messaging environment. Resending sensitive information text-to-text with the non-secure texting client is not appropriate – see Option 4.

- Option 2 – Copy/Paste information from the standard client into the County provided secure text environment and send it to appropriate personnel.

- Option 3 – Email Transfer. (When the information received requires retention, but retention is not sensitive.) – Select and copy the message content, paste it into an e-mail addressed to County e-mail account, send the e-mail, and retain it in your email archive in accordance with the applicable document retention schedule. The e-mail automatically records the date, time, and message recipient identity. Resending sensitive information text-to-email is not appropriate. – see Option 4.

- Option 4 – Manual. Transcribe the message content and retain such transcription(s) in accordance with the applicable document retention schedule. Record the date, time, and identity of the message recipient in the transcription. This is the only appropriate option for retaining sensitive information received outside of the secure texting service as it avoids the rebroadcast of sensitive information in plain text format.

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

For documents, photographs, audio, video, and other files that constitute public records, that are created or updated on a mobile device, transfer all such files as e-mail attachments to the User's County e-mail account and retain them in accordance with the applicable document retention schedule. If the files are too large for an e-mail attachment, contact the IT Help Desk for assistance.

5. Guidelines for Safeguarding Text Messages Containing Protected Information.

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's secure text message solution.

5.2. Ensure the device is password protected and is configured to timeout after no more than 10 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, contact the ITS Helpdesk during business hours or the Sheriff's Office Records Division after-hours.