ADMINISTRATIVE POLICIES

SECTION: 600 – Information Technology	**POLICY#:** 601
TITLE: Texting Policy	**R & O #:** 16-136
	IMPLEMENTED BY PROCEDURE #: 601-A
SPONSORING DEPT/DIV: Department of Information Technology Services (ITS)	
ADOPTED: 10/18/2024	**REVIEWED: 2/12/2026**

PURPOSE: This policy establishes guidelines for using text messages for business purposes, ensuring compliance with public records and confidentiality laws. Although texting is a convenient and widely used form of communication, it must be conducted with care and in accordance with public sector regulations and best practices. All other forms of instant messaging for business purposes that occur outside of County-controlled infrastructure are prohibited.

AUTHORITY:
This Policy will be administered by the County Administrative Office in accordance with Section 34 of the Washington County Charter and the authority delegated to the County Administrator in Washington County Code Section 2.04.100.

APPLICABILITY: This policy and County Administrative Procedures No. 601-A and B apply to:

1. This policy applies to all individuals who use or connect to the County's network and systems, including but not limited to elected officials, employees, volunteers, interns, consultants, and contractors (collectively, referred to herein as 'Workforce members')

2. All information technology owned or managed by the County, as defined below.

    a. Technology Owned or Managed by the County as referenced herein includes, but is not limited to, the following:

        i. All electronic information and communications created, processed, or stored on networks and devices owned or managed by the County.

All electronic information and communications relating to County business, regardless of where such records are stored, including on personally owned devices or in personal emails, in portable

storage media, or in the "cloud."

DEFINITIONS:

1. **Restricted Data** means it is classified as restricted when the unauthorized disclosure, alteration, and/or destruction of that data could cause a critical level of risk to the County. Protected or Sensitive Data is classified as Restricted Data.

    - Examples: Social Security Numbers, Personally Identifiable Information (PII), Protected Health Information (PHI), and financial records.

2. **Confidential Data** means it is classified as confidential when the unauthorized disclosure, alteration, and/or destruction of that data could result in a moderate to high level of risk to the County. This includes, by default, all County data that is not explicitly classified as restricted or public data. Private data is classified as Confidential Data.

    - Examples: Internal business documents, employee performance reviews, and strategic plans.

3. **CIS Controls:** The County uses the Center for Internet Security (CIS) Controls to guide its cybersecurity practices. These controls are a set of recommended actions that help protect County systems and data from cyber threats.

4. **Encryption:** Encryption protects data in storage and during transmission. Encryption plays a crucial role in cybersecurity by safeguarding information from interception or misuse by unauthorized parties. Adequate protection requires adherence to encryption standards and secure transmission protocols.

GENERAL POLICY: The County permits workforce members to use text messaging when it improves process efficiency and timely communication.

All text messages related to County business are considered public records, and workforce members must retain them in accordance with public records retention requirements.

If a text message contains Restricted Data, you are required to use the County's secure text messaging application, which provides encryption and supports compliance with applicable laws and regulations. This text messaging application must be used on any device, County-owned or personal, when conducting County business that involves restricted information.

POLICY GUIDELINES:

1. <u>Responsibilities</u>:

    (a) The Information Technology Services (ITS) shall:

i. Be responsible for developing procedures to implement this policy.

ii. Ensure that the relevant CIS controls for technology owned or managed by the County are in place to protect the security of text messages.

(b) Workforce members shall:

i. Be responsible for using the County's secure text messaging protocols as required by this policy and adhering to Public Records retention requirements.

2. Exceptions: May only be granted by the Washington County Board of Commissioners unless such authority has been delegated to the County Administrator.

3. Implementation: Elected officials and department directors are expected to review, understand, and implement this policy within their respective departments. Adherence to this policy is mandatory for all County employees and volunteers. Any violations of this policy may result in disciplinary action, up to and including termination.

4. Periodic Review:

ITS shall review and update this policy at least every two years, or more often if necessary.