Title: **Mobile Device Policy**
Policy Number: **305**
Effective Date: **July 1, 2009**
Revision Date: **August 28, 2018, July 9, 2020**
Authorized by: **Board of Supervisors**

POLICY

Mobile devices such as cell phones and tablets may help employees to more effectively perform their jobs, but they also create new risks to privacy, confidentiality, intellectual property and protected health information ("PHI") in the workplace. This policy is intended to manage the risks that mobile devices present in the workplace.

SCOPE

This policy applies to all county employees and Elected Officials. Exceptions may be made for law enforcement or emergency reasons.

DEFINITIONS

Mobile Device – Any electronic computing and communications device used by an employee that is capable of receiving, processing, or transmitting digital information in any manner. ***Mobile devices include cell phones, smartphones, mobile computing and communications devices, digital music players, hand-held computers, laptop computers, tablet computers, personal digital assistants (PDAs) and similar devices.***

Prohibited Mobile Device – Mobile devices which have not been configured to comply with this policy or which may produce electromagnetic interference with medical devices, equipment located in county medical clinics (public health or county jail) or communications equipment (communications center or remote sites) are prohibited.

Business Use – Any call, text, email, internet connection or similar action taken by an employee for the purpose of conducting official county business in direct support of their assigned duties and responsibilities.

Personal Use – Any call, text, email, internet connection or similar action taken by an employee when not conducting official county business.

Confidential or Sensitive Information – All information collected or created by an employee should be treated as confidential. Confidential information includes, but is not limited to the following:

- Protected Health Information (PHI), as defined under HIPAA or other medical information protected by state or federal law.
- Confidential personal or county information, such as employee records, social security numbers, driver's license numbers, and financial information.
- Photographs or video showing patient faces or building security measures.

- Metadata, data that is created and collected by a mobile device, while conducting official county business.
- Intellectual property such as software designs, copyrighted text, logos or graphics.

Security Officer – An individual appointed by the Board of Supervisors who is responsible for overseeing, implementing and monitoring the security requirements for the County's HIPAA program.

Privacy Officer – An individual appointed by the Board of Supervisors who is responsible for overseeing, implementing and monitoring the County's HIPAA program.

MOBILE DEVICES IN THE WORKPLACE – GENERAL USE

General Policies:
Use of mobile devices must comply with this and other county policies. The use of mobile devices may be terminated by the county at any time for any reason. Work performed on a mobile device is considered as hours worked. Non-exempt (hourly) employees, who are not "on-call", shall not perform work, i.e. answer texts, emails during non-working hours unless they have express permission to work overtime from their supervisor.

Personal Phone Calls/Text/Email/Internet Usage:
Personal use of a mobile device (calls, text, email, or internet usage) during the work day should be limited to break or lunch times to the maximum extent possible. Employees are not allowed to distract other employees with use of their personal mobile device at work. The Elected Official or Department Head, at his/her sole discretion, is permitted to ban or limit employees' use of personal mobile devices at work.

Confidential Records:
Various records created or maintained by Pottawattamie County contain confidential and sensitive information such as medical and mental health information, personally identifiable information such as names, dates of birth, telephone numbers and similar information as well as photographs and videos of individuals. This information must be handled in strict accordance with this policy. Storage and transmission of confidential or sensitive information on a mobile device, whether by email, internet or wireless means, is prohibited unless the device is registered with IT and the transmission is encrypted as set out in this policy.

Business Use of Mobile Device and Cellular Phones
If an Elected Official or Department head requires that the employee be accessible for county business, the employer may issue the employee a county owned mobile device for work.

Mobile devices purchased and issued by the county shall remain the property of Pottawattamie County. Employees may be responsible for any costs associated with replacing a lost, stolen or damaged county-issued mobile device due to employee carelessness or negligence. Employees should not use a county-issued mobile device for personal use unless authorized by their Elected Official or Department Head. Employees may be responsible for charges incurred by the county for an employee's personal use of the county-issued mobile device. Records contained on or about a county-issued mobile device, such as cellular phone records, may be considered public records and may be subject to Iowa Open Records laws.

Employees provided county-issued cellular phones are expected to be accessible, on and off duty, as required by the Elected Official or Department Head.

Reimbursement for Business Use of Personal Cellular Phones

Elected Officials may receive a reimbursement for the business use of their personally-owned mobile cellular device. The Board of Supervisors shall determine the reimbursement level on an annual basis during the first meeting in January. The Elected Official is required to register their personal cellular phone with IT for access to county systems and shall provide documentation of the actual monthly cost of the mobile device such as a monthly statement or invoice to be eligible to receive a monthly reimbursement.

Elected Officials or Department Heads may provide a reimbursement to their employees for talk and text use of their personal cellular phones during a designated time period where the employee experiences a high call volume for work related issues. Reimbursement for talk and text use shall not exceed $20.00 per month and the employee is required to submit a copy of their monthly phone bill in order to receive reimbursement.

All county-related communication conducted on an employee-owned device may be considered a public record and may be subject to relevant provisions of Iowa Open Records laws.

Mobile Device – Access to County Email, Data and Computer Systems/Programs:

Elected Officials and employees who access county email, networks, data and similar systems (county systems) on a mobile device are required to register the device with the Information Technology (I.T.) Department. Authorization to register the mobile device must be in writing by the Elected Official or Department Head and must be approved by the county Security Officer.

Before access is granted to county systems, the I.T. Department shall confirm the following:

- Receipt of written authorization to register the mobile device.
- The device is password protected as required by policy.
- Encryption software has been installed on the device.

- Anti-virus application/software has been installed on the device.
- Location services for the applicable device applications have been enabled.

Employees are prohibited from accessing county systems with an unregistered mobile device. Accessing, transmitting or disclosing confidential or sensitive information by a mobile device must be in compliance with all Pottawattamie County policies at all times.

Confidential and sensitive information stored on the mobile device or transmitted from a mobile device must be encrypted and the mobile device must lock after unsuccessful login attempts and timeout access to the mobile device based inactivity. Bluetooth and infrared (IR) services must be configured as approved by the Security Officer or turned off.

Lost or Stolen Mobile Device:

Employees granted access to county systems containing confidential and sensitive information are required to report a lost or stolen mobile device immediately to the Elected Official or Department Head **AND** to the County's I.T. Department. The I.T. Department will immediately disable the mobile device access to county systems and attempt to locate the device. If the mobile device was not password protected and the employee had access to confidential or sensitive information with the mobile device, the Security Officer may authorize the wiping or erasing of the mobile device data to factory settings to avoid a security breach.

Suspension of Mobile Device Access to County Systems:

Access to county systems may be suspended at any time with or without notice to the employee based on the needs of the county. Suspension from county systems will occur if one of the following takes place:

- If the employee fails to password protect their mobile device or refuses to comply with any section of this policy or any other similar policy.
- To avoid, prevent or mitigate the consequences of a violation of this policy.
- To investigate a security breach, security incident, or violation of this or any other county policy or policies.
- To protect individual health, privacy, reputation or financial interests.
- To protect any county assets, information, reputation or financial interests.
- Upon request of the Elected Official or Department Head in which the employee works.
- Upon request of the County Attorney's Office or the Security or Privacy Officer.

Termination of Mobile Device Access to County Systems:

Access to county systems may be terminated at any time with or without notice to the employee. Termination will occur if one of the following takes place:

- Upon separation of employment with Pottawattamie County.
- Upon a change in the employee's role, as directed by the Elected Official or Department Head in which the employee works.

- If it is determined that the employee violated this or any other County policy affecting the use of a mobile device.
- The use of a mobile device without authorization, while authorization is suspended, or after authorization has been terminated is a violation of this policy.
- Upon request of the Elected Official or Department Head in which the employee works.

Employees shall return all county-issued mobile devices and county equipment upon termination of employment or upon direction of the Elected Official or Department Head.

Internal Audit of Mobile Devices:
The encryption software application required on mobile devices that have access to county systems or that contain confidential or sensitive information will automatically perform audits of the registered mobile device to ensure the device is password protected. The encryption software will also scan the mobile device for applications and services that may be harmful to device security and may prevent the installation of the application. If this occurs, authorization for installation must be approved by the county's Security Officer.

An audit may be performed by the county at any time to ensure compliance with this and other county policies. Employees are required to cooperate with an audit request. Employees shall not delete or modify any confidential or sensitive information stored on the mobile device after receiving an audit request.

Audits or Evidentiary Review – Use of Personal Information:
All information on a mobile device registered on the county system, including personal information, may be subject to audit or "evidentiary review" as provided in this policy. Any personal information may be used or disclosed by Pottawattamie County to the extent necessary.

Evidentiary Review of Mobile Device:
As part of a complaint or lawsuit, it may be necessary to preserve evidence that may be contained on an employee's mobile device. If so, the Pottawattamie County Attorney's Office will request that the employee submit their mobile device for an evidentiary review to determine if the mobile device contains evidence relevant to the complaint or lawsuit. Employees are required to cooperate with any request for an evidentiary review by the Pottawattamie County Attorney's Office. An employee receiving such a notification shall immediately turn their mobile device over to the County Attorney's Office and shall not delete or modify any confidential or sensitive information that may be stored on the mobile device after receiving the request for an evidentiary review.