Policy: Mobile Device Policy
Reference No. FIN-008
Original Adoption: June 2015
Updated: May 13, 20262026

Policy Statement

The City of Mound's Mobile Device Policy defines the standards on appropriate business use of electronic communication devices operated onsite and offsite that are connected to the City of Mound network. Devices which are provided by the City of Mound and personal devices utilized to carry out City of Mound business are covered by this policy.

This Mobile Device Policy includes, but is not limited to cell phones, smart phones, iPads, and tablets. All employees, contractors, part-time, temporary, and volunteer workers, and those employed by others to perform City of Mound work remotely or who have been granted access to City of Mound information or systems are covered by this policy and must comply with all related standards, policies, and procedures.

Policy Overview

Authorization

All device connections to the City of Mound network must be coordinated through Administration / IT.

The Deputy City Manager or the IT Consultant has final authorization of all devices connected to City of Mound networks and may be withdrawn at any time. Authorization will be based on the following improvements or needs:

- Safety
- Emergency contacts
- Communication
- Work efficiency

Non-exempt employees require prior authorization from Human Resources to conduct City business outside of their workday. This applies to all devices and includes checking City email accounts, working on City related documents and any other type of City related communication.

Expectations of Use

- Use of mobile devices must follow all applicable laws and regulations.
- Employees cannot use the device while operating a City motor vehicle or power equipment with the exception of fire personnel utilizing a device during active operations.
- Under no circumstances may an employee use the City's devices for any personal income-producing work. This will be subject to disciplinary action.

- Limited personal use of City of Mound systems is acceptable as long as it does not conflict with City of Mound business and interests.
- Any use perceived to be illegal, harassing, offensive, to reflect badly on the City of Mound, or interfere with normal business operations will be considered a violation of this policy. Examples of such violations include but are not limited to: sexually explicit material, political activities, material supporting intolerance or disrespect.
- Users are responsible for all activity connected with their account(s) and assigned equipment.

Right to Monitor

Employees should have no expectations of privacy when using a device connected to City of Mound systems.

- All information created, received, processed, sent, and/or stored on City of Mound networks is City of Mound information assets and property.
- The City of Mound reserves the right to monitor, record, and audit use of any of its systems and equipment, both those owned by and connected to the City of Mound's systems. Use of these systems and equipment implies consent to such monitoring, recording, and auditing.
- The City of Mound reserves the right to disclose any user's activities involving City of Mound systems and equipment to law enforcement officials or other third parties without any prior notice to the user.

Security

- All devices must be protected with a power-on passcode, whenever technologically possible.
- Account passwords are confidential. Passwords must not be shared and should be protected. Passwords should not be stored in obvious locations such as on a device screen or in its case.
- When not on your person, devices should be physically secured and locked if possible.

Storing and Transferring Documents

- Electronic communication that constitutes an official record of City business must be kept in accordance with all records retention requirements and should be copied to the appropriate location for storage.
- Restricted or confidential data must not be stored on mobile devices.

City-Owned Devices

- Only City employees or authorized contractors may use City-owned equipment. Family members or friends of employees are not allowed to use City equipment or technology resources.
- The City reserves the right to remotely wipe any and all data on a City-owned device at any time. If there is any personal data on the device such as contacts or photos, it is the employee's responsibility to transfer and save the data to an appropriate personal storage location. Although IT will attempt to take measures to prevent data loss, the City is not responsible for any lost data when the device is wiped, updated, tested, or restored to its original state.

- Malfunctioning or damaged City-owned devices must be reported to department directors and IT within 24 hours.' Report compromised, lost, or stolen devices to your direct supervisor and the Deputy City Manager and/or IT consultant within 24 hours.

Applications

- All software applications purchased and installed by City of Mound must remain on the City-owned device.
- Storage space on devices needed for City of Mound applications will take priority over space used for personal items.
- Employees are allowed to request applications to be used for business purposes on City-owned devices. IT will coordinate the purchase and installation of all applications. Applications may be denied and can be removed at any time if known to or suspected to, interfere in any way with City-owned equipment and data.
- The City of Mound is not responsible for the loss of any application data when the device is updated, tested, or restored to its original state.
- IT will be responsible for and troubleshoot any applications required for all City-owned devices to install such as Email and VPN connectivity. Limited support will be available for all other applications.

Availability

- The device should be maintained, charged and accessible during assigned work hours and standby periods.

- Required protection mechanisms must not be removed or disabled from city-owned devices. Examples include but are not limited to network cards, GPS location, Mobile Device Management (MDM) agent, and power-on passcodes.

Ownership

- Purchase of mobile devices must be authorized by the Deputy City Manager and coordinated through IT. Department Heads are also responsible for maintaining a list of all City-owned mobile devices and related service assigned to employees in their department and must update IT of all changes.

- The City of Mound's mobile devices, and information produced and stored on City devices are the sole property of the City. The City has exclusive rights to review, retain, maintain, modify or delete these files, messages and documents. This includes personal messages, photos, and any other files that reside on City equipment and storage media. Employees may not distribute or copy City data without proper authorization.

- City owned equipment must be returned when the employee leaves City of Mound employment.

Personal Devices
By opting to use a device for personal purposes, employees waive any claims to privacy regarding their usage.

Access to the City of Mound's network and data from a personal device may be revoked at any time if the device is known to or suspected to interfere in any way with City-owned equipment and data.

Applications

- City funds may not be used to purchase applications for personal devices, with the exception of the Dialpad app.

Data

- Storing City data, including documents, messages, and photos, on a personal device is strictly prohibited.

- Employees may be required to provide their personal mobile device as part of a discovery request. This may be related to a discovery request involving records accessed by or stored on an employee's personal device of where the employee has used their personal device to access the City's network to receive work related documents (including emails and texts).

Reimbursement

- The City of Mound will reimburse employees for the use of personal devices used for official City business when approved by their Department Head.

- Reimbursement rates will be determined during the previous year's budget cycle by the Human Resources division, communicated to all applicable employees, and changed on all appropriate forms.

- Employees with a cell phone reimbursement are responsible for all costs related to the cell phone plan they choose. For example, lost or stolen phones that break or quit working, plan penalties, activation fees, and excess charges are all the responsibility of the employee. The City of Mound is only responsible for the approved "cell phone reimbursement."

<u>Roles and Responsibilities</u>

A. **Human Resources** is the approval authority for the policy.
B. The **Deputy City Manager** and the **IT consultant** are the final authorization of all devices connected to the network and is responsible for coordinating access to the City's network.
C. **Department supervisors** are responsible for notifying the Finance Department of when reimbursement should be started or suspended.
D. **City of Mound Department Directors** are accountable for ensuring that the Mobile Device Policy is properly communicated and understood within its respective units. City of Mound Department Directors are also responsible for defining, approving, and

implementing procedures in their respective units and ensuring their consistency with the Mobile Device Policy.

E. **Employees** agree that any access to a secure network will meet the secure networks security requirements and restrictions.

Enforcement and Exceptions Handling

Failure to comply with the *Mobile Device Policy* and related guidelines and procedures can result in disciplinary actions, up to and including termination of employment for employees, and/or termination of contracts for contractors, partners, consultants, and other entities. Legal actions may be taken for violations of applicable regulations and laws.

Related Procedures:

- Request Form for City-owned Mobile Device and Service
- Request Form for Personal Mobile Device Use and Reimbursement

Approved: /s/ Jesse Dickson

City Manager