Mobile Device Policy	
Original Adoption: 06/23/2015 Reviewed/Updated: TBD	Reference No. FIN-008

Purpose - The City of Mound recognizes that investments in mobile device technology improves efficiency and effectiveness of its employees, particularly those in the field and whose responsibilities continue after the normal work day. This policy sets forth the conditions under which mobile devices and corresponding usage charges will be funded.

Business Use Justification Requirements – Cellular telephones, laptops and Ipads are provided for official City business use and are made available to employees in positions where the associated benefits justify the additional operating costs. Employees who travel or have job responsibilities that include being outside of the office or are continuously on call for extended periods may be good candidates for a City-funded mobile devices.

Individual Assignment and Self-Management – Employees will acknowledge the receipt and acceptance of the conditions for the individual assignment of a City-owned mobile device by signing a copy of the Mobile Device Agreement Form. Department heads are responsible for keeping the Agreement Form on file for the duration of the individual assignment of a mobile device. When the employee leaves his/her position or is no longer an authorized user, the City mobile device must be returned to the employee's supervisor or other designated official.

Public Information – Call detail (e.g., time, number called, date, duration) of calls appearing on the City cellular telephone billing account is public information, except when exempt by statute.

Use of City Cellular Telephone for Personal Calls – The use of City-owned cellular telephone equipment and service is intended for City business. Personal use of City-owned cellular phones is allowable only for incidental use.

Incidental Personal Calls – Incidental personal calls are defined as meeting the following requirements:

- minimum duration
- minimum frequency

Examples of incidental personal calls include but are not limited to calls to arrange for care of a child or other family emergency, to alert a family member of an unexpected delay due to a change in work schedule, or to arrange for transportation or service in the event of car trouble.

Reimbursement and Possible Disciplinary Action – Employees are expected to use City cellular telephones responsibly and in accordance with this policy and any applicable work rules. Personal use of a City cellular telephone in violation of this policy or agency work rules may result in revocation of the cellular telephone assignment and possible disciplinary action against the employee.

Monthly Cellular Bill and Annual Service Reviews – Employees are responsible for paying any excess over the basic plan amount unless a higher minute or data plan is approved for the position, then the employee is responsible for any amount of the set plan approved by the City Manager. Accounts Payable will bill the employee for the excess charges and the employee is responsible to submit payment within 5 business days. Departments should conduct a review annually of the individual cellular telephone assignments to determine if there is a continuing need and if it is cost justified.

Number Portability – In the event of a change of vendors for the city's cellular contract, the cellular numbers may be ported (transferred) from one vendor to another. Porting a personal cellular number to a city billing account is prohibited, as is porting a city cellular number to a personal billing account. This will avoid commingling personal and business calls.

Employee Safety – All City of Mound employees shall adhere to the following Federal Law.

Federal law prohibits commercial vehicle drivers from the use of hand-held mobile phones while driving. The ban prevents commercial motor vehicle drivers from holding, dialing or reaching for hand-held cell phones, including phones with the push-to-talk function. Drivers are also banned from using phones while at traffic stops unless they have moved their vehicles off the road. Hands-free use of devices with either a wired or wireless earpiece, or the use of the speakerphone function, is permitted.

Security. Notebook computers, USB flash drives, and other removable media devices are often used outside a secure network environment, which makes them particularly susceptible to loss. As a result, extra care needs to be taken to protect the devices and any "not public" data contained on them.

All computers should be secured with a strong password. To protect both the data and the computer equipment, the following security measures should also be considered:

- Government data should not be stored on personal computers, personal USB flash drives, and other similar personal equipment.
- "Not public" data should be stored on a notebook computer or removable media device only when there is a business need.
- Data stored on a notebook computer or a removable media device should be strongly encrypted.
- When removable media are no longer in use, they should be securely destroyed.
- When disposing of computers, the hard drives should be securely erased or destroyed.
- Cable locks should be used for all computers, except while in transit.
- Computers should never be left in an unattended vehicle.

City Cell Phone Allowances effective January 1, 2012	Verizon
Call & Data plans	
Basic Plan (400 minutes no texting)	$35
Americas CH Email & Data (1000 minutes unlimited data)	$75
PIX Message – 20 message bundle	$ 3
Phones – Blackberries are not permitted due to software requirements for Microsoft Exchange	
Basic Phone for Public Works -	

OSA 2/13/15 **Avoiding Pitfalls: Security for Portable Computing and Media Devices**

Notebook computers, USB flash drives, and other removable media devices are often used outside a secure network environment, which makes them particularly susceptible to loss. As a result, extra care needs to be taken to protect the devices and any "not public" data contained on them.

All computers should be secured with a strong password. To protect both the data and the computer equipment, the following security measures should also be considered:

- Government data should not be stored on personal computers, personal USB flash drives, and other similar personal equipment.
- "Not public" data should be stored on a notebook computer or removable media device only when there is a business need.
- Data stored on a notebook computer or a removable media device should be strongly encrypted.
- When removable media are no longer in use, they should be securely destroyed.
- When disposing of computers, the hard drives should be securely erased.
- Cable locks should be used for all computers, except while in transit.
- Computers should never be left in an unattended vehicle.

The State of Minnesota's Information Technology organization, MN.IT Services, has a number of resources on their website for governmental entities who are drafting security policies for portable computing and media devices. To view this material, go to:

http://mn.gov/mnit/programs/policies/security/.