



To: Mayor and City Council

From: Dylan Mulfinger

Subject: City Cell Phones

Date: 2/8/2021

The City does not have a consistent policy or standard when it comes to cell phone usage or reimbursement within the organization of the city. Employees who are required to have a cell phone are sometimes reimbursed, or their phone is provided by the City. The City Administrator recommends the following to bring a standard practice to the City:

- Require that all employees who must have a city cell phone carry city issued phones.
- City issued phones can only be used for city related purposes.
- The City will no longer reimburse City employees for use of their personal phones.
- Employees who carry a city phone must respond within a reasonable time frame.

7.13 Electronic Communication Systems/Personal Use Policy in the City's Personnel Manual provides direction for employees of proper use of their City phone. City Hall will manage the city's cell phone plan and will adjust as needed.

At this time City Council would consider a motion to update the city's cell phone policy. The City will no longer offer reimbursements and will only provide a phone as determined by the City Administrator.



Policy already existing in the City's Handbook. The changes below will be made upon council formally approving a new cell phone policy.

7.13 Electronic Communication Systems/Personal Use Policy

(A) Purpose: To better serve the City's citizens and give the City's workforce the best tools to do their jobs, the City continues to adopt and make use of new means of communication and information exchange. This means that many City employees have access to one or more forms of electronic communications systems, including, but not limited to computers,¹ computer files, e-mail, telephones, cellular or "cell" phones, pagers, voice mail, fax machines, external electronic bulletin boards, wire services, media services, on-line services, applications including social media such as Facebook, the Internet, and the World Wide Web (hereafter "electronic communication systems").

The City encourages the use of electronic communication systems because it is an efficient and effective way to facilitate and support City business and to stay abreast of the latest information relevant to the City and its customers. The City's electronic communication systems are the City's property and there shall be no expectation of privacy regarding their use. This includes use of personal devices over the City's electronic communications systems.

The purpose of this policy is to express the City's philosophy and set forth general guidelines governing the use of electronic communications systems. By adopting this policy, it is the City's intent to ensure the electronic communication systems are used to their maximum potential for City purposes and not used in a way that is disruptive, offensive to others, or contrary to the best interests of the City.

(B) Applicability: This policy applies to all City departments, offices, boards, commissions, committees, City employees and contracted and consulting resources.

This policy applies to all electronic communication systems that are:

- Accessed on or from City premises or City systems (i.e., wireless internet systems, server systems, etc.);
- Accessed using City owned or paid-for electronic communications systems; or
- Used in a manner that identifies the individual as acting for or on behalf of the City; or in any way identifies the City.

(C) Policy: It is the policy of the City to follow this set of procedures for the use of electronic communication systems. If any electronic device provided by the City is lost or stolen, employees must report the loss or theft to their immediate supervisor who will report the loss or theft to the

¹ Desktop, lap top, tablet or other hand held devices and external hard drives.



City Administrator. If the immediate supervisor cannot be contacted, employees should make every reasonable effort to immediately contact the City Administrator.

As City-owned electronic devices are decommissioned or replaced, employees shall turn them in, including all accessories, attachments and cases, to their immediate supervisor, who will forward them to the City Administrator.

Malfunctioning electronic devices shall be reported to the immediate supervisor for reporting to the City Administrator.

Department Heads or their designees are responsible for notifying the City Administrator for discontinuing, canceling or changing electronic devices or services when an individual employee voluntarily or involuntarily terminates his/her employment with the City or if some other change is made which discontinues an employee's use of an electronic device.

Employees shall surrender all electronic devices upon termination to their immediate supervisor. If an employee fails to surrender an electronic device assigned to them by the City upon termination of his/her employment, the fair market value of the City-owned electronic device will be withheld from the employee's final paycheck pursuant to Iowa Code § 91A.5. See Acknowledgment form for express authorization for this withholding.

~~(D) Reimbursement for Personal Electronic Devices Used for City Purposes~~

~~The City, through the City Administrator may provide a reimbursement for personal cell phones or other electronic devices in lieu of providing a cell phone or other electronic devices to conduct City business. The above policy applies regarding proper use of personal cell phones or other electronic devices when used for City business and where the City reimburses employee for said devices.~~

~~By using a personal electronic device for City business, employees are acknowledging that the records and information contained on the personal electronic device or in the billing for the personal electronic device may be public records pursuant to Iowa Code Chapter 22.~~

(E) Access and Authority

Each Department Head shall determine which employees in their department shall have access to the various media, applications, and services, based on business practices and necessity and which shall have authority to communicate on behalf of the City with approval of the City Administrator/Mayor.

Electronic information created and/or communicated by an employee using the City's electronic communication systems may be monitored, intercepted, accessed or preserved by the City for any purpose including, but not limited to: cost analysis; resource allocation; optimum technical management of information resources; and detecting use which is in violation of City policies or may constitute illegal activity. Employees shall have no expectation of privacy using the City's electronic communication systems, including in situations where an employee is using a personal



device over a City electronic communication system. Disclosure of electronic information will not be made except when necessary to enforce a policy, as permitted or required under the law, or for other legitimate business purposes.

Any such monitoring, intercepting and accessing shall observe any and all confidentiality regulations under federal and state laws.

City-owned electronic communications systems may be removed from City premises solely for City work-related purposes pursuant to prior authorization from the immediate supervisor.

Most of the City's computing facilities automatically check for viruses before files and data which are transferred into the system from external sources are run or otherwise accessed. On computers where virus scanning takes place automatically, the virus scanning software must not be disabled, modified, uninstalled or otherwise inactivated. If an employee is uncertain as to whether the workstation the employee is using is capable of detecting viruses automatically, or the employee is unsure whether the data has been adequately checked for viruses, the employee should contact the City Administrator.

(F) Prohibited Communications/Uses

The City's electronic communications systems and the employee's personal electronic communications systems being used during working time shall not be used for knowingly transmitting, retrieving or storing any communication that is:

1. Personal business on City time (e.g. sports pools, games, shopping, correspondence, supplemental employment or other non-City-related items), except as otherwise allowed (see Personal Use section);
2. Discriminatory or harassing;
3. Derogatory to any individual or group;
4. Obscene as defined in case law and under Iowa criminal law;
5. Defamatory or threatening;
6. Using another individual's account or identity without explicit authorization;
7. Attempting to test, circumvent, or defeat security or auditing systems without prior authorization;
8. Accessing, retrieving or reading any e-mail messages sent to other individuals without prior authorization from the City Administrator;
9. Permitting any unauthorized individual to access the City's e-mail system;
10. Engaged in for any illegal purpose or one contrary to the City's policies or best interests;
11. Sent in an attempt to hide the identity of the sender or represent the sender as someone else; and
12. Likely to cause network congestion or significantly hamper the ability of other people to access and use the system.

Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by the City Administrator, employees are prohibited from engaging in, or attempting to engage in:

1. Monitoring or intercepting the files or electronic communications of other employees or third parties;



2. Hacking or obtaining access to systems or accounts they are not authorized to use;
3. Using other people's log-ins or passwords; and
4. Breaching, testing or monitoring computer or network security measures.

City employees shall not download or transfer software unless authorized by the immediate supervisor. Employees must understand that the unauthorized use or independent installation of non-standard software or data may cause computers and networks to function erratically or improperly, or cause data loss. Users must never install downloaded software to networked storage devices without the assistance and approval of the immediate supervisor.

Body Worn Video (BWV) and other audio/visual recording devices shall only be used in conjunction with performance of official, authorized, sanctioned and assigned job duties. See applicable department standard operating procedures.

Activation of recording devices such as microphones, cameras and video to record communications with any other person outside of departmental standard operating procedures while at work or on City business is prohibited where such activity violates another employee's or another person's rights to protect their confidential personnel or medical information or where the information would otherwise qualify as a confidential record under Iowa Code Chapter 22.

(G) Acceptable Communications/Uses

Except as otherwise provided, electronic communication systems are provided by the City for employee business use during City time. Limited, occasional, or incidental use of electronic communications systems (sending or receiving) for personal non-business purposes is permitted as set forth below:

1. Personal use is limited to breaks, lunch or immediately before/after work;
2. Personal use must be brief and must not interfere with the productivity of the employee or co-workers;
3. Personal use shall not involve any prohibited activity (see Prohibited Communications/Use section above);
4. Personal use does not consume system resources or storage capacity on an ongoing basis;
5. Personal use does not involve large file transfers or otherwise deplete system resources available for business purposes;
6. The City's phone numbers and email address **shall not** be listed in any publication or electronic communication that will result in personal incoming phone calls, text messages or other forms of electronic communications.
7. Non-City personnel are not authorized to use the City's electronic communication systems except in an emergency.
8. Anyone obtaining electronic access to other organizations', businesses', companies', municipalities' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.
9. Anyone receiving an electronic communication in error shall notify the sender immediately. The communication may be privileged, confidential and/or exempt from disclosure under applicable law. Such privilege and confidentiality shall be respected.



(H) Confidential Information

All employees are expected and required to protect the City's confidential information. Employees shall not transmit or forward confidential information to outside individuals or companies without the permission of their immediate supervisor and the City Administrator.

The City also requires its employees to use e-mail in a way that respects the confidential and proprietary information of others. Employees are prohibited from copying or distributing copyrighted material - for example, software, database files, documentation, or articles - using the e-mail system.

(I) Policy Violations

Employees who abuse the privilege of City-facilitated access to electronic media or services risk having the privilege removed for themselves and possibly other employees, are subject to disciplinary action up to and including termination and may be subject to civil liability and criminal prosecution