PHOENIX FIRE DEPARTMENT

VOLUME 1 – Operations Manual

ELECTRONIC COMMUNICATIONS AND INTERNET USAGE POLICY

MP102.12 06/19-R

PURPOSE

This MP, in conjunction with City AR 1.63, will provide the guidelines for using electronic communications. E-mail, Internet and Intranet are important tools that assist us in providing excellent customer service to the public as well as our internal customers. City electronic property or electronic communications systems should not be used for personal gain, including personal businesses, but rather to enhance service to the public. Harassment and pornography will not be tolerated. Jokes, junk mail, chain letters and other non-work related items should not be sent or forwarded.

CITY POLICY

All hardware, software, databases, email, mailbox messages, spreadsheets, files and documents are the electronic property of the City of Phoenix.

Employees should be aware that they are responsible for any information that they generate or distribute through the electronic system.

Employees are expected to prevent the unauthorized use of the City's internet and E-mail systems while logged into the City's network by using password–protected screen savers or other appropriate techniques while away from their computer. **Any use that occurs on an employee's workstation under that employee's login is presumed to be performed by that employee. Log off the computer when you're not using it.**

Policy Statements

1 **City Workforce Accountability.** All members of the City workforce are accountable for the security of their user IDs and passwords, and for all actions performed by their computer accounts. City workforce members may not use another's user ID and password, nor allow another to use their user ID and password.

2 **Privacy Expectations.** The City workforce has no expectation of privacy for any electronic information created, received, stored in, or transmitted on the City's electronic property or electronic communication systems.

In accordance with Arizona's Public Records Law, the public may request all information made or received by City workforce in performance of their jobs. The City workforce must consider all information, including email and City information residing on personal devices, open to public view unless the Law Department determines there is a specific legal confidentiality requirement.

3 Use of Personal Devices. As described below, the City workforce may use personal devices for work involving information classified as public. Reference: s1.9 Information Classification Standard.

City workforce members performing any work on personal devices are encouraged to connect to the City's network using the City's remote access facility to best protect City information. To help ensure compliance with Public Records Law, the City workforce should not store any City information on a personal device or system.

While City workforce members may use personal devices to access their City email as stated below, they should not conduct City business using personal email accounts.

City workforce members may not use personal devices for work involving any personal identifying or restricted City information that may result in* a *critical breach of information security. Reference: A.R. 1.90 Information Privacy and Protection.

The City workforce may not use personal devices to access Criminal Justice Information unless specifically authorized by the City's Criminal Justice Information Services (CJIS) Officer. The CJIS Officer must approve and authorize any access, processing, storage, or transmission of Criminal Justice Information using personal devices.

3.1 Use of Personal Devices for Messaging. The City workforce may use personal devices, such as smartphones for telephone, texts, and email related to City business. While the City workforce must comply with all other provisions in this AR., no additional approvals are required.

3.2 Use of Personal Devices for Messaging and Offline Work. The City workforce may use personal devices, such as pad and/or tablet computers for texts, email, and work related to City business without connecting to the City's network. This in.eludes accessing email via a web browser. While the City workforce must comply with all other provision in this AR., no additional approvals are required.

3.3 Use of Personal Devices Connecting to City Network. The City workforce may use personal devices, such as pad, tablet, laptop, or desktop computers to connect to the City's network with approval from their department's information security liaison and with the understanding that the City may require City-provided and monitored management software to ensure compliance with City policies.

4 Required Training. The City workforce must complete all applicable information security awareness training within the timeframes that the City establishes. This includes, but may not be limited to new hire and annual training.

5 **Security Software.** The City workforce must not disable or circumvent any software or controls intended to safeguard City information systems.

6 **Unattended Devices.** The City workforce must appropriately protect all unattended information systems and promptly report any suspicious activity that may affect information security, or the loss or theft of a device containing City information to their department's information security liaison.

7 **Authorized Software.** The City workforce must use only City-authorized software on City-owned devices. The City workforce may neither use nor distribute unauthorized software in the course of performing City business. Reference: AR 1.86 Legal Use of Software.

8 **Copyrights and Licensing.** The City workforce must always comply with all applicable copyright and license requirements. Reference: AR 1.86 Legal Use of Software.

9 **Records Management.** The City workforce must comply with all records retention policies and schedules.

The City workforce must not delete and/or modify any electronic records in a manner that violates their approved retention periods and/or any other legal requirements. For example, members of the City workforce must not empty their email system trash or modify activity logs. Reference: AR 1.61 Records Management Program.

10 **System Use.** The City workforce must use City information systems and protect City information in accordance with all A.R's and standards. Reference: A.R 1.84 Information Security Management.

11 **Ownership.** The City owns all information residing on its information systems. Upon termination of City employment, contract, or agreement, City workforce members must return all equipment, software, and information, whether in electronic form or otherwise.

12 **Personal Use.** The City workforce may use City information systems for incidental personal use as long as it

- Consumes only a minimal amount of computer system resources or staff time
- Does not interfere with productivity or any business activity
- Does not cause the City to incur additional costs
- Does not require repeated and ongoing use or registration of their City email account, as City workforce members should not use their City email address as their primary personal email account
- Does not violate any City AR. or standard, or any applicable law or regulation, and
- Would not adversely affect the reputation of the City, its citizens, or its employees.

IV. PRIVACY AND MONITORING

The City reserves the right to monitor systems, electronic communications, and usage to support operational, maintenance, auditing, security, and investigative activities, including enforcement of this policy, legal requests, public record requests, and to help ensure and to verify compliance, confidentiality, integrity, and availability of information systems used to conduct City business. This AR does not prohibit technical staff from monitoring departmental workstations and servers for the purpose of maintaining overall system reliability, availability, and security. Unauthorized accessing, monitoring, or reading of electronic communication systems or their contents violates this City policy.

Between the City and its employees and other individuals using the electronic property or electronic communication systems, the individual user has no expectation of privacy. By using the city's electronic property or electronic communications system, each user acknowledges that the city may monitor all such uses. The user specifically consents to the city performing the monitoring function.

In accordance with Arizona's Public Records Law, the public may request all information made or received by City workforce in performance of their jobs. The City workforce must consider all information, including email and City information residing on personal devices, open to public view unless the Law Department determines there is a specific legal confidentiality requirement.

The city does not monitor the content of city electronic property, electronic communications or internet access as a routine matter, but reserves the right to do so without notification.

Only Department/Function Heads or higher may request access and monitoring of City electronic communication for employees under their supervision. Details for such requests are outlined in City of Phoenix Administrative Regulation 1.63.

PROHIBITED ELECTRONIC PROPERTY AND ELECTRONIC COMMUNICATIONS USES

Prohibited uses include, but are not limited to:

- Any personal use that interrupts City business and that keeps an employee from performing his/her work. Employees should not use their City e-mail account as their primary personal e-mail address.
- Extensive personal use of the internet for any non-work- related purposes during working hours which decreases employee productivity or results in decreased performance of the City's e-mail system.
- Unauthorized downloading and distributing of copyrighted materials (e.g. music, pictures or other proprietary information).

- Downloading or copying music, including music obtained legally, for non-business purposes onto city computers or servers.
- Unauthorized reading, deleting, copying, modifying, or printing of electronic communication of another user.
- Using the city's electronic connections for private gain or profit (e.g. online gambling, personal business, etc.).
- Instant messaging through public service providers. (e.g. AOL, Yahoo, MSN, etc.).
- Personal software, which allows peer to peer communications between two or more workstations. (e.g. online chat, KaZaA file sharing, etc.).
- Personal use of the City's electronic connections for auctions such as eBay.
- Soliciting for political, religious or other non-business uses not otherwise authorized by A.R. 2.33
- Non –business related streaming media (e.g. listening to internet radio stations).
- Using City computers for political purpose, including voting. This does not include using equipment designated for public voting at city facilities.
- Sending or forwarding junk email, chain letters, or mass mailings.
- Theft and /or forgery (or attempts) of messages or electronic documents.
- Using, accessing, or transmitting pornographic or sexually explicit materials, offensive threatening, racial, or hate language or images.
- Engaging in any form of harassment, whether sexual or otherwise, or sending any unwelcome personal communication. It is the perception of the recipient that prevails, not the intention of the sender.

~~PRIVACY AND MONITORING~~

~~Between the City and its employees and other individuals using the electronic property or electronic communication systems, the individual user has no expectation of privacy. By using the city's electronic property or electronic communications system, each user acknowledges that the city may monitor all such uses. The user specifically consents to the city performing the monitoring function.~~

~~In accordance with Arizona's Public Records Law, the public may request all information made or received by City workforce in performance of their jobs. The City workforce must consider all information, including email and City information residing on personal devices, open to public view unless the Law Department determines there is a specific legal confidentiality requirement.~~

~~The city does not monitor the content of city electronic property, electronic communications or internet access as a routine matter, but reserves the right to do so without notification.~~

~~Only Department/Function Heads or higher may request access and monitoring of City electronic communication for employees under their supervision. Details for such requests are outlined in City of Phoenix Administrative Regulation 1.63.~~

RETENTION AND STORAGE

The City is required by Records Retention Policy to maintain electronic mail for one month. Email in the trash basket falls under the one-month retention policy. **Employees must not empty their electronic mail trash and must ensure that electronic systems are set appropriately to preserve messages for 30 days.** The City Clerk Department is responsible for purging electronic mail from the Domino/Lotus Notes Enterprise Email system older than one month.

VIOLATION OF POLICY

Violation of these policies is cause for disciplinary action.

CITY OF PHOENIX

ELECTRONIC COMMUNICATIONS AND INFORMATION ACCEPTABLE USE

CITY WORKFORCE RECEIPT

This form must be signed by each current and new member of the City workforce.

I acknowledge that I have received A.R. 1.63, Electronic Communications and Information Acceptable Use. I recognize that as a user of City information, electronic communications, and computer systems I am responsible for following the provisions outlined in this policy. I understand that if I am found to be in violation of this written policy, I may be subject to disciplinary action.

Name (printed)_____

Signature_____ Date_____

c: Copy to individual member of the

City workforce

Original to department file