THE CITY OF LAKE FOREST **ADMINISTRATIVE DIRECTIVE 2-4**
Office of the City Manager **May 2019**

ELECTRONIC COMMUNICATION SYSTEM POLICY

1.0 Purpose:

1.1 General Purpose

This policy establishes standards for the acceptable use of the electronic communications system of The City of Lake Forest (City), including smartphones. It is established in recognition of the City's significant investments in the system for the purposes of more effectively and efficiently providing City services. These service goals can only be achieved through the careful and thorough protection of the system for all users. It is therefore essential to establish standards for responsible use of the system.

1.2 Generally Acceptable Uses

Users of the Internet, email, and all other forms of external communication, including social networking sites, are representatives of the City. Use is restricted to activities required to perform the duties of a City employee's position.

1.3 Unacceptable Uses

1. Users must not use the Internet for purposes that are illegal, unethical, harmful to the City, or nonproductive.

2. Unacceptable uses include but are not limited to: conducting personal business using City resources; unproductive use of time like online shopping or internet surfing; anything that will compromise or cause down time of any City asset; and transmitting any content that is defamatory, offensive, harassing, discriminatory, disruptive, derogatory, fraudulent, anything that violates the City's anti-harassment policy or any other inappropriate use.

2.0 Scope:

All elected officials, appointed officials, fulltime, part-time, temporary employees, and contractors.

3.0 Policy:

3.1 Responsibilities of All Users

1. All users shall take care to use only appropriate language, behavior and style at all times.

2. All electronic use and messages regarding City business are considered City records and may be regarded as public information. The City reserves the right to access the contents of all messages sent over its electronic communication system, including Gmail, Yahoo, Hotmail and AOL accounts, if the City feels there is a business need to do so. Users cannot assume any privacy regarding the content of electronic communications. The City may review messages at any time to enforce this policy, to

prevent harassing or threatening messages, for investigations, and for security/system/audit checks and maintenance.

3. Although data and electronic communications are backed up and/or archived by the Information Technology Division (IT), it will be the responsibility of the user to retain a copy of any electronic correspondence that may be classified as a public record under the Illinois Freedom of Information Act (FOIA), to the extent that that law applies. All FOIA requests are administered by the City Clerk. Users are required to comply with any request from the City Clerk in order to comply with FOIA requests.

4. Application downloads or installations on any City asset are not permitted under any circumstances without prior written approval from IT. This includes, but is not limited to, software applications or upgrades, multimedia streaming applications, messaging software, free/shareware, and file sharing applications. Exclusions may include employees who have been pre-established as an administrator responsible for a specific system in order to perform this function. Apps on City-provided Smart phones/tablets may be downloaded by the primary user without permission from IT. It is the responsibility of the employee to maintain their smartphone or tablet in good operating condition.

5. Each user shall be responsible for all computer transactions that are made with his/her user ID and password. Passwords will not be disclosed to others and will be changed immediately if it is suspected that others may know them. Passwords must not be recorded where they can be easily obtained.

6. User passwords are required to be changed on a regular interval and also meet complexity requirements based on best practice. Password resets and expired passwords are to be managed through the City's Password Reset Utility.

7. Users must lock the workstation they are using before leaving the it unattended. When leaving a workstation unattended for an extended period, users must log off their user account. Workstations should be turned off at the end of the work day.

8. Those employees with administrative responsibilities on City systems shall have a secondary account for administrative access only. This secondary account is subject to a stricter password complexity requirement.

3.2 Management Responsibilities

Managers and supervisors must ensure that all personnel are aware of and comply with this policy. Managers and supervisors must create appropriate performance standards, control practices and procedures designed to provide reasonable assurance that all employees observe this policy. They are responsible for assuring proper use by their employees.

3.3 Mobile Communication Equipment and Mobile Storage Devices

1. Global Positioning System (GPS): Cellular communications or third party applications may access the GPS embedded within a mobile device on an emergency basis or for a pre-established business need.

2. Privacy Notice: Wireless systems use radio channels to transmit communications that may be accidentally or intentionally intercepted. Although federal and state laws make it illegal for third parties to listen in on the City's Service, privacy cannot be guaranteed.

3. Any mobile device capable of accessing or storing City data must be locked with an access code, personal identification number (PIN), or password to prevent unauthorized access.

4. It is the responsibility of the user to protect any mobile communication device or removable data storage media protect from environmental hazards and unauthorized access.

5. IT shall make every reasonable effort to encrypt mobile data storage devices to prevent access by an authorized party.

4.0 Procedures:

4.1 Access Codes and Passwords

1. IT shall be responsible for the administration of access controls to all City computer systems. Changes may be requested to IT through the IT helpdesk system or password reset utility.

2. Remote access by employees and third parties must be requested to IT through the Remote Access Request form and approved by the department head of the sponsoring department.

4.2 Malicious Software

1. Malicious software includes but is not limited to; viruses, worms, trojans, adware, spyware, ransomware, key logging, and sniffing utilities.

2. IT shall take all reasonable precautions against infection of workstations and all other IT assets from malicious software using actively updated anti-virus software, firewalls, and other methods of intrusion prevention. Specific files that become infected will be attempted to be cleaned. Files that cannot be cleaned will be automatically deleted. Systems found to be infected will be removed from the network until such time as the system is rebuilt.

3. Network monitoring, intrusion detection, incident logging, and response coordination necessary for the detection, elimination, and recovery from various forms of attack on City resources is managed by the IT Division.

4.3 Copyrights and License Agreements

All users are legally bound to comply with the Federal Copyright Act and all propriety software license agreements. Noncompliance can expose the City and the responsible user to civil and/or criminal penalties.

The IT Division will maintain records of software licenses owned by the City and periodically scan City computers to verify that only authorized software is installed. Any unauthorized/illegal/non-supported software will be immediately removed.

4.4 Computer Acquisition Policy

All technology hardware, software, and/or hosted/outside service purchase must be properly justified, reviewed by IT, and approved by the City Manager according to Administrative Directive 3-5, Purchasing Procedures. The IT staff will assist in acquisition to insure system compatibility.

4.5 Discipline

Violations of this policy will result in disciplinary action to be determined by the Director of Human Resources and the City Manager based on the type, severity and other circumstances surrounding the violation, up to and including termination. The City's possible tolerance of prior policy violations is no defense against disciplinary action under this policy.

5.0 Forms and Resources

IT has developed guides to further assist employees. All can be found on the IT Shared folder on SharePoint. Examples of resources currently available:

1. User Account Request Form
2. New Employee Guide
3. Password Reset Guide
4. Employee Pre-Purchase Technology Request Form
5. Employee Remote Access Form

6.0 Distribution

Human Resources website, www.citylf.org.

Jason Wicha
City Manager

adopted 5/97
revised 5/99, 5/01, 5/05, 5/11, 5/14, 5/19