	ADMINISTRATIVE ORDER	Approved By: City Manager	No. #9 **Effective Date**: 01/21/2003 **Revised:** 12/01/2010
Subject**: Electronic Communications**			

INTRODUCTION

The City of Highland Park's ("City/City's") information technologies provide valuable opportunities for the City. These technologies, when properly used, support the City's activities and enable City employees to better serve the community through enhanced communication and nearly instantaneous access to vast resources of information. In recognition of these benefits, the City has made a substantial investment in its Information Systems ("System"). While the City encourages the use of its technology, such use carries with it important responsibilities. Careless or inappropriate use can have dramatic consequences and compromise the integrity of the System. This policy is intended to minimize the likelihood of such harm by educating users as to proper and improper use of such Systems and by setting forth the conditions that apply whenever the City's computer, e-mail, Internet tools and cellular telephones are being used.

DEFINITIONS

1. "Access" shall mean the ability to read, change relocate or delete the City's Information Systems.

2. "E-mail" shall mean the electronic document, file, and message distribution capabilities in the System; the transmission or receipt of any oral, written, or visual communication, image, or sound through the System; and the communication or image itself whether in electronic form or any other reproduction of it.

3. "Internet" shall mean the interconnected worldwide network of computers generally open and available for access by any person, typically through the use of a browser.

4. "Information System" ("System") shall mean the City's computer network, hardware, and software including, but not limited to, e-mail, web page, and Internet access and including all documents and

5. “System Administrator” shall mean the City Manager and any designee authorized by the City Manager to act on the City Manager’s behalf.

6. “Telecommunications” shall mean City phone system, City-issued cell phones and pagers, personal cell phones used for City business.

7. “Third Party Services” shall mean Internet or telephone services provided by an entity other than the City that permit Users to read, transmit, download, receive, or post written or visual information, such as discussion groups, electronic mailing lists, bulletin boards, personal messenger, and chat rooms.

8. “Users” shall mean all elected and appointed officials of the City and all employees of the City including full-time, part-time, temporary, and seasonal employees and any other person authorized to use the System.

9. "Online Communication" means all methods of communication utilizing the Internet besides e-mail access provided by the City and includes, but is not limited to, web-based forms and applications, chat rooms, instant messaging, electronic bulletin boards and forums, voice over IP and third-party e-mail services.

MANAGEMENT AND ADMINISTRATION

The City of Highland Park’s Information Systems, e-mail, and Internet access are provided for official City business. The City of Highland Park maintains software that can monitor and record all Internet usage. The City retains the right to record each website visited, newsgroup, e-mail message or file transfer at any time. Any abuse or violation of the policies outlined herein will be brought to the attention of the applicable Department Director and may result in disciplinary action.

NO PRESUMPTION OF PRIVACY; CITY’S RIGHT TO MONITOR INFORMATION SYSTEMS, E-MAIL, INTERNET ACCESS

The use of passwords or User accounts to access the System is designed to inhibit unauthorized access by outside third parties, not to provide personal privacy. The System Administrator shall have the right, but not the duty, to monitor, access, retrieve, examine, intercept, block, and delete any files, e-mail, Internet use and resources on the System. This may be done without prior notice to the individual user, senders or recipients of any e-mail, including, but not limited to the following circumstances:

- When the System Administrator suspects that a user has engaged, or is about to engage, in inappropriate conduct while using the System, including violations of this usage policy or any other City Administrative Order or policy;
- When required by law or in order to protect the City's own interests.
- When the user in question is unavailable (e.g., ill, on vacation or leave, no longer working for the City);
- When the System Administrator otherwise determines that it is in the best interest of the City to do so.

The System Administrator may also disclose such information (without prior notice to the User or the senders or recipients of e-mail) to law enforcement officials, to other third parties when the City is legally required to do so, and to third parties and authorized City personnel where required for business purposes. Without limitation, the City may also monitor Internet activity, including websites, chat rooms, video streaming and newsgroups accessed by users.

Primary Use for Job Responsibilities. Each User shall use, operate, and allow for the operation of the System primarily in furtherance of the User's job responsibilities.

Incidental Personal Use of the System. Incidental personal use of the System shall be permitted, provided that such incidental personal use (i) complies with the limitations set forth in this Policy; (ii) does not interfere with the User's duties and responsibilities to the City; and (iii) does not place any burdens on, or interfere with, the primary purpose of the System.

INFORMATION SYSTEMS USE

The City currently has a computer infrastructure in place that spans workstations, servers, network printing devices and fiber data network. These Systems run vast amounts of applications that assist employees in conducting City business. All users share in the responsibility to protect the City's Information Systems from physical and environmental damage. The following guidelines are in place to maintain the integrity of the System:

1. The City owns the hardware and software resources that comprise the City's Computing Environment. The term "Computing Environment" includes the physical and logical networks, servers, personal computers (networked and stand-alone), storage, network-attached telephones, software and related equipment. The term "Computing Environment" does not include equipment owned by individual City employees or other third parties, which equipment may be used by such employees or third parties to access the City's Computing Environment after permission is granted by the System Administrator. Devices provided by the City that interact with

the City's computing environment, including wireless devices such as notebook computers, personal digital assistants (PDAs) and data-enabled cellular telephones (smart phones), are considered part of the City's computing environment.

2. The City retains the right to determine if and in what manner personally-owned devices are allowed to interact with the City's Computing Environment. There is no obligation on the part of the City to allow interaction with any specific personally-owned device type, make or model. Where interactions are allowed between personally-owned devices and the City's Computing Environment, there is no obligation on the part of the City to support proper functioning of the personally-owned device.

3. Individual computer usernames and passwords are initially provided to new users by the Systems Administrator at the request of the Department Director or Human Resources Division. Employees are required to change their individual passwords on an established basis. Users are required to access the System using their own individual accounts unless utilizing a shared System. Users shall not disclose their account passwords, unless such request to do so is made by a supervisor or the System Administrator.

4. All City computers have security in place to protect confidential information. Computers are password protected. Users will not enable unauthorized third parties to have access to or use the System, or otherwise jeopardize the security of the System (this includes access by the User's spouse and children). Workstations should not be left unattended. If the User is not in physical control of the workstation, they should lock or log off of the workstation. All Users will be responsible for any violations of the City's Electronic Communications Policies that occurs when registered to that username and password.

5. Filtering and monitoring software is installed on the network. The City reserves the right to monitor data, documents, and electronic mail (e-mail) messages at any time without prior notice to the user. Computer Services may periodically audit the storage devices of all computers and reserves the right to clear any and all data not related to City business.

6. All data, files, programs, application software, documents, e-mail, and any other electronic information stored on any System owned by the City is considered City property. This includes all programs licensed by the City for its use. As City property, all data, files, programs, application software, documents, e-mail, and any other electronic information are subject to inspection for the purposes of determining their compliance with this and other City policies.

7. A user may not utilize the City's System to create, send, receive, access, or store any of the following unless deemed necessary as part of an official

City investigation with prior written approval of a Department Director or the City Manager's Office:

- Copyrighted, trademarked, or patented material; trade secrets, or other confidential, private, or proprietary information or materials in violation of the law;
- Illegal information or materials;
- Any information (including messages, images, video, or sound) that a reasonable person would consider to be of a harassing, intimidating, offensive, malicious, violent, hateful, sexually explicit, illegal, or discriminatory nature. The provisions of the City's Employee Handbook related to sexual harassment, discrimination, and other prohibited conduct shall apply to all uses of the System.

8. Hardware or Software may only be loaded onto City computers if its use has been approved by the System Administrator and Department Director and is licensed by the City. In the event the System Administrator becomes aware of non-City hardware or software loaded on a City computer, notice will be made to the employee's applicable Department Director for approval or direction to remove the hardware/software.

9. No data, files, programs, application software, documents, e-mail, nor any other electronic information for City business will be copied or transferred from the System for personal use. Unauthorized copying of these items may constitute theft and can be subject to disciplinary action or criminal prosecution.

10. Only files related to City business may be stored and backed-up on the City's servers. Digital movies, games, sound, picture or music files for personal use are not authorized to be stored on the City servers. Files stored on individual City computers will not be backed up.

11. All disks, tapes, or data obtained from outside the System must be checked for viruses before they can be used in the System. If assistance is required in this regard, the System Administrator should be contacted.

12. Computer problems should be brought to the attention of the user's supervisor, who will evaluate the problem and make arrangements for its repair, if necessary.

13. The City Manager's Office is the primary Department responsible for updating the City's website. Staff with access to direct access to the website shall reside in the City Manager's Office and include the following employees: City Manager, Deputy City Manager, Assistant City Manager, Management Analyst and Administrative Interns. All other employees who are required to update the City's website shall use the content management system. It is the discretion of the System Administrator and

immediate supervisors as to which employees are eligible to post to the website.

E-MAIL USE

"E-mail" are text documents, which are created, stored and delivered, in an electronic format. As such, e-mail messages are similar to other forms of communication such as letters, memoranda and other internal staff memos.

1. Authorized users are provided a login name and personal password that allows access to the System. The confidentiality of this password will be the sole responsibility of each user and users will not disclose their password to other users. Any communications via the E-mail System will be attributed to and the responsibility of the login name of the originating user.

2. The City reserves the right to access and review the contents of any employee's electronic mailbox, including deleted messages without prior notice to the employee. Such access may occur, but is not limited to the City's need to investigate a suspected violation of policy or breach of the Computer or Electronic Mail System Security. Any contents obtained under these guidelines may be disclosed on a need-to-know basis without the consent of the employee.

3. To maintain the security of the System, each user shall be required to lock the System when they are not in physical control of the computer.

4. Caution must be exercised when receiving an e-mail message from an unknown source. The potential to spread viruses is significant, and opening an infected message, especially an attachment, could have devastating consequences for the System. If the user is unsure and cannot verify the message is safe, it should be deleted without opening.

5. Certain information on the Internet may be protected by copyright laws. The E-mail System shall not be used to obtain, store, or use illegal copies of copyrighted materials. This prohibition includes, but is not limited to, illegal copies of music, videos, or software. Illegal copies of software or content are subject to immediate confiscation and/or deletion upon discovery. If users are unsure whether a document or information is protected by copyright laws, they should consult their supervisor.

6. Users shall not allow an unauthorized person, employed or not employed by the City, to access their established e-mail account for any reason. Any user found to have engaged in unauthorized access

or attempted unauthorized access to another user's e-mail account may be subject to discipline.

7. The use of City e-mail to initiate mass-mailings not related to City business is prohibited.

8. The use of City e-mail to access or attempt to access, transmit, store, display or request obscene, pornographic, erotic, profane, racist, sexist or other offensive material (including messages, images, video or sound) is prohibited.

9. The E-mail System may not be used for commercial activities, religious, charitable solicitations, support for outside organizations, or other activity not related to the direct conduct of official City business. Any use of the City e-mail to solicit support or to advocate for any political causes, outside organizations or other non-job related purposes, including, but not limited to, those Politically Prohibited Activities listed in Section 37.003 of the City Code, is prohibited.

10. Any e-mail transmissions to an external party that incorporate any statement concerning the City of Highland Park, its position on any issue or policy, comments on any pending case or legal action, comments requiring a legal interpretation or policy making decision are strictly prohibited except as authorized by the City Manager's Office.

11. It is the responsibility of each employee to check his or her City e-mail account for messages during work hours. By opening the document, the employee is indicating that he or she has received and read the document. If the user has questions regarding the document, they should be brought to the attention of his or her immediate supervisor. Responses to e-mail communications should adhere to the City's Customer Service Protocols for written communications (located in hpshare/customerservice). Police Patrol Officers and Operational Field Personnel are responsible for checking their email once during their shift. All other employees are responsible for checking their e-mail account, at a minimum, at the beginning, in the middle, and before the end of their shift. Exempt employees shall check their e-mail account within the hours of their designated shift.

12. Mobile e-mail access to the City network is provided for City business during normal business hours. While it is recognized that work-related e-mail may arrive at any hour, non-exempt employees are encouraged to refrain from addressing work-related messages during that time. Exempt employees may access mobile e-mail in order to monitor the status of projects and work-related activities.

13. Employees seeking access to retrieve filtered e-mail messages, documents and attachments should contact the System Administrator. An employee requires the consent of the immediate supervisor and the System Administrator in order to gain access to blocked emails. The employee will need to demonstrate the reason for obtaining these e-mails on a permanent basis.

E-MAIL AND ONLINE COMMUNICATION RECORDS RETENTION

Purpose

This policy establishes standards for the retention of records generated using the computer and online communications system of the City of Highland Park. This policy is established in recognition that e-mail and other forms of online communication may result in the creation of records that are subject to local, state and federal laws applicable to public records, including among others, the Illinois Freedom of Information Act (5 ILCS 140/1 *et seq.*), the Illinois Local Records Act (50 ILCS 205/1 *et seq.*), and the Illinois Open Meetings Act (5 ILCS 120/1 *et seq.*). In addition, such records may be subject to discovery in federal and state court litigation.

The Internet is evolving constantly in form and content. It is impossible, therefore, to anticipate and describe in this policy all of the forms of communication a User may engage in when using the City's computer and online communications systems. Accordingly, it is the policy of the City that all use of, and conduct on, the City's computer and online communications systems shall be governed by the same policies, principles, and law which guide users in other work activities.

E-mails and Online Communications identified as Public Records must be retained for the same amount of time that a paper copy of the same Public Record would be retained as required by the most recent disposal schedule issued to the City by the Illinois Local Records Commission.

"*Public Records*" means any book, paper, map, photograph, digitized electronic material, or other official documentary material, regardless of physical form or characteristics, made, produced, executed or received by any agency or officer pursuant to law or in connection with the transaction of public business and preserved or appropriate for preservation by such agency or officer, or any successor thereof, as evidence of the organization, function, policies, decisions, procedures, or other activities thereof, or because of the informational data contained therein. (Illinois Local Records Act, 50 ILCS 205/3).

Because of the precise and tedious nature of records retention, and in an effort to assist the City in complying with the State of Illinois FOIA

requirements, the City utilizes an e-mail archiving application that archives all incoming, outgoing and internal e-mail communications that go through the City's network. Employees will not be initially responsible for determining if an e-mail meets the definition of a public record, or the timeframe in which it must be maintained. The City will comply with the Illinois Public Records Act by following the timeframe for the longest applicable retention period. The system will allow for ease in searching for public records in response to FOIA requests in a timely manner so that the stringent response deadlines placed on the City may be met. The message archiver will initially copy all existing records stored in the City's exchange system. This includes calendar entries, tasks, contacts and e-mails (including sent items, deleted items retained in the deleted item folder, and e-mails stored in any subfolders that have been created by each user). Attachments to these entries will be archived as well. In addition to the existing records stored by users, the message archiver will begin to create copies of all e-mails sent to and from any City of Highland Park e-mail address, including e-mails sent internally between City staff members and City officials using a City e-mail address. The system will also store any calendar, task list or contacts entries created, as well as changes and deletions of these items.

Since the City will archive all e-mails for the longest retention period applicable per the Illinois Public Records Act, the City advises and encourages employees to limit the receipt and transmission of personal e-mail communication in order to preserve space for e-mails that pertain to the City of Highland Park. Employees with questions regarding e-mail record retention should contact their Department Director.

INTERNET USE

Internet usage is granted to employees to enhance their knowledge and their ability to effectively and efficiently conduct City business. It is imperative that use of the Internet be conducted in a professional, courteous and ethical manner at all times.

1. Use of the Internet by City employees shall be in compliance with all applicable laws and policies. The Internet shall not be used for any illegal, improper, unprofessional or illicit purposes. Any commercial use of the Internet for personal gain, violations of copyright laws, or illegal activity is prohibited. The use of the Internet to access or attempt to access, transmit, display or request obscene, pornographic, erotic, profane, racist, sexist or other offensive material (including messages, images, video or sound) is prohibited. Intentional misuse may subject the user to termination of access rights, disciplinary action and/or criminal charges.

2. A wide variety of information is available on the Internet. Some individuals may find some information offensive or otherwise objectionable. The City has no control over and cannot therefore be responsible for the content of information available on the Internet.

3. Many sites on the Internet are sources for computer viruses. Computer Services has taken every precaution to limit the threat of virus infections; however, caution at every user access point is warranted. If a virus is detected, users must promptly notify their immediate supervisor.

4. Personal Internet use by employees during work hours is limited to breaks and meal times. At no time may personal Internet usage conflict or interfere with the employee's duties or otherwise compromise his or her job duties.

5. Digital recordings of any type that are not work-related may not be downloaded or streamed from the Internet due to their impact on the System bandwidth unless permission is granted by the Department Director or Systems Administrator.

6. The City maintains the right to monitor and block the activities of employees while accessing or using the Internet, and to review the contents of stored records. Any attempt to circumvent these monitor control features is a violation of this policy. Violation of City policy regarding Internet use may result in disciplinary action up to and including termination.

7. Employees seeking access to filtered Internet websites should contact the System Administrator. An employee requires the consent of the Department Director and the System Administrator in order to gain access to blocked websites. The employee will need to demonstrate the reason for obtaining access to blocked websites on a permanent basis.

TELECOMMUNICATIONS

The City organization exists to serve all the residents of the City of Highland Park. Each time an employee answers a City telephone, it is an opportunity to fulfill the City's mission to provide excellent customer service. Employees should answer each call respectfully and in a pleasant manner. This is often the first impression that a person has of the City organization. Regardless of the circumstances, each person deserves courtesy, tact and fairness.

Every employee is responsible for ensuring that each call leaves a favorable impression by:

- Taking time to learn the features and proper operation of the City's Telephone System;
- Becoming familiar with the City organization and individual departments. This will enable employees to be of greater assistance to the caller;
- Reading and understanding the City's Telephone Procedures (see Personnel Handbook);
- Adhering to the City's Customer Service Protocols (located in hpshare/customerservice).

TELEPHONE RESPONSIBILITY

Employees may not make personal long distance calls while at work unless a personal credit card is used or the call is charged to the employee's home telephone number. Personal phone conversations while at work should be limited to break times and shall not conflict or interfere with the employees' duties or otherwise compromise their ability to do their job.

Those employees who are issued City cellular telephones are accountable for calls made independent of City business. City cellular telephone includes regular cellular phones and "smart" cellular telephones with Internet and e-mail accessibility. The City recognizes that personal calls may be conducted from a City-issued phone both during normal business hours and outside of normal business hours. Personal calls should be made with sound judgment and in a responsible manner.

The use of 411 and other types of informational services for which there is a charge, including reverse look up, should be limited to situations where all other possible means of obtaining the necessary information have been exhausted or it is an emergency where time is of the essence.

All communications via voicemail, telephone, or facsimile transmission, regardless of the business or personal nature of the communication, created, transmitted, received, stored, or maintained using any of the City's telephone systems are subject to being accessed and reviewed by the City, without prior notification to the individual user.

USE OF CELLULAR TELEPHONES AND DATA DEVICES

A. Purposes

It is the policy of the City to provide a safe and healthful work environment for its employees and, to the extent reasonably possible, to prevent injury to employees and third-parties to the extent possible while employees are performing their work functions. This policy is intended to control the manner and means under which any employee may utilize a cellular telephone during hours of work in order to:

i) Minimize the risk of an accident occurring while an employee is operating a vehicle on City business, and

ii) To ensure that City resources are utilized appropriately.

Employees may be authorized and required to operate a licensed motor vehicle in order to perform their work activities. This policy is intended to control the manner and means under which any employee may utilize a cellular telephone for a telephonic conversation, whether such telephone is issued by the City or personally owned by the employee, during the time period when the employee is authorized and required to operate a licensed motor vehicle in order to perform work activities. This policy also stipulates the use of a cell phone while on duty.

B. Policy

1. If the City has issued a cellular telephone to an employee, the employee is authorized to use the City-issued cellular telephone for reasonable personal purposes during working hours and non-working hours, so long as its use does not interfere with assigned work functions. If the City has issued a cellular telephone to an employee, or provides a cellular telephone for use by an employee, the employee is authorized to use the phone during all working hours, including overtime, weekends, special events and in emergencies.
2. Employees driving a City-owned vehicle and using a cellular phone must adhere to applicable state and local laws and ordinances with respect to traffic regulations and restrictions.
3. The acquisition of cellular phones and supporting equipment shall be limited to those instances where there is a demonstrated need for equipment in order to perform essential City business or to improve safety, increase productivity, increase service to the public, or where necessary communications cannot be provided by any other means. The purchase of cellular phones shall be subject to the approval of the appropriate Department Director.
4. City-issued smart phones with Internet and e-mail capability shall be reserved for Senior Executive and Management Staff members, unless otherwise approved by the appropriate Department Director with consent of the City Manager for an extenuating circumstance. An exception would require substantial justification from the Department Director as to why an employee other than a Senior Executive and Management Staff member would require a cellular phone with data capabilities. The designated J.U.L.I.E. staff liaison is the only employee who is not a Senior Executive and Management Staff member authorized to receive a cellular phone with e-mail capability. All distributed smart phones are required to be compatible with ActiveSync.
5. Issuance and/or reassignment of cellular phones for new employees, for employees who are leaving the City, transferring internally, changing work addresses or phone numbers, as well as assigning of or changes to cellular phones for current employees, must be authorized by the

appropriate Department Director and communicated to the Management Analyst. Employees are not authorized to switch phones or SIM cards with other employees. All questions pertaining to cellular phone maintenance should be directed to the Management Analyst.

C. <u>Guidelines</u>

1. The City reserves the right to monitor employee compliance with this policy through appropriate means, including, but not limited to, vehicular surveillance, monitoring of conversations, and auditing of records reflecting use of cellular telephones during the employee's working hours. By accepting a City-owned cellular telephone or utilizing a personally-owned cellular telephone during working hours, the employee consents to the City's right to conduct monitoring to determine employee compliance. City-issued cellular phones stationed in shared vehicles may be subject to audit; however, given that these are community phones, such a process must take into account that various employees are utilizing the device and an immediate supervisor must have substantial justification to demonstrate an employee is utilizing the shared phone in an inappropriate manner.

2. This policy is intended to comply with existing federal, state or local laws and regulations that may control the usage of a cellular telephone during the operation of a vehicle on City business and during working hours. The City reserves the right to amend or modify this policy at any time to comply with any such federal, state or local law or regulation that controls the usage of cellular telephones while on City business and during working hours. This policy shall be deemed to be amended or modified to comply with such federal, state or local law or regulation that controls the usage of cellular telephones while on City business and during working hours.

3. Carrying of cellular phones or pagers by members of the Fire Department or Police Department while on-duty shall be pursuant to Fire Department Policy #8 and Police Department General Order #153, respectively.

4. While at meetings, training sessions, or similar events where a ringing phone would be considered a distraction, City-issued cellular telephones and personal cellular phones should be placed in the silent/vibrate mode; answering of calls or monitoring of messages must be limited to appropriate circumstances. Employees are asked to use discretion when answering calls from either a City-issued cellular phone or personal cellular phone during work hours depending on the circumstance and location.

5. Employees whose job responsibilities do not specifically include driving as an essential function, but who are issued a cellular phone for business use, are also expected to abide by the provisions above. Under

no circumstances are employees allowed to place themselves at risk to fulfill business needs. Employees are expected to comply with all applicable state and local laws pertaining to the operation of vehicles.

6. Employees who are charged with traffic or other violations resulting from the use of City-issued cellular phones while driving a personal vehicle will be solely responsible for all liabilities that result from such actions. Employees who are charged with traffic or other violations resulting from the use of City-issued or personal cellular phones while driving a City-issued vehicle will be solely responsible for all liabilities that result from such actions.

7. A City-issued cellular phone's camera can be utilized for work purposes and personal use. Any picture that is taken with a City-issued camera phone, personal or work related, shall be utilized with discretion.

8. Employees who use a personal cellular phone rather than a City-issued cellular phone will not be reimbursed for phone calls, e-mails, text messages or any other form of communication pertaining to City business.

9. The City will not port City-issued telephone numbers to an employee's personal cellular phone.

VOICEMAIL SYSTEM

The City provides voice mailboxes for its employees. This resource is an essential and necessary component in the City's ability to function efficiently and effectively. Police Patrol Officers should refer to General Order #65: Department Voicemail System for correct procedures. Operational Field Personnel are responsible for checking voicemail once during their shift. All other employees are responsible for checking their voicemails, at a minimum, at the beginning, in the middle, and before the end of their shift. Exempt employees shall check their voicemail within the hours of their designated shift. When on vacation or unavailable for a period of more than one business day the greeting message should be changed to inform callers of the employee's absence and who the caller may contact during that time. No employee may access another employee's voice mailbox without prior approval from his or her Department Director. The City reserves the right to access and inspect the contents of an employee's voice mailbox without prior notice to the employee.

TELEPHONE SERVICE REQUESTS

Any change of service regarding the Telephone System such as new extensions, additional extensions, change of extension designations etc., must be requested in writing from the department director, or designee to the System Administrator.

SOCIAL NETWORKING

Employees who choose to engage in social networking websites outside of employment hours shall use discretion when associating oneself with the City of Highland Park. Employees shall avoid conduct that would compromise the integrity of the City or undermine the mission statement set forth by the City. Additionally, employees who desire to use the City logo, photos, video recordings, and related materials must seek approval and advanced written permission of their Department Director before proceeding.

REPORTING MISUSE OF SYSTEM BY OTHERS

Misuse of the City's systems may occur in various forms. Employees are responsible for reporting violations of this Order to their immediate supervisor.

DISCIPLINARY ACTION

Failure to follow this policy will result in disciplinary action up to and including termination.

TERMINATION OF EMPLOYMENT

Department Directors are responsible for immediately informing the System Administrator upon notification that an employee will no longer be employed with the City. This will grant the System Administrator sufficient time to remove employee access from the System at the time of departure.

INTERPRETATION

All questions pertaining to the meaning or applicability of this policy should be submitted in writing to the City Manager's Office. The City Manager's Office will provide a written interpretation to all departments, which will serve as a supplement to this policy. The City Manager and Finance Director reserve the right to audit the actions of any persons designated as the System Administrator under Administrative Order #9 at any time.