

(5)

MEMO

TO: DEPARTMENT DIRECTORS, AGENCY HEADS, MEMBERS OF BOARDS AND COMMISSIONS, CITY COUNCIL MEMBERS, AND THE CITY CLERK

FROM: Information Technology Services Department
Human Resources Department

DATE: June 26, 2000

SUBJECT: DIRECTIVE FOR THE USE OF THE CITY OF DETROIT'S ELECTRONIC COMMUNICATIONS SYSTEM

1. Scope

Due to the City's increased use of electronic technology, the City is establishing this directive for the creation and use of its electronic communications system, including electronic mail ("e-mail"). This Directive, which is subject to modification at any time, shall govern the use of the City's electronic communications system by all City employees, in-house contractors, independent contractors, interns, students, volunteers, and other persons having authorized access to, and using any of, the City's electronic communications system. The City's electronic communication system includes Intranet and Internet e-mail, internal electronic bulletin boards, Intranet and Internet services, news groups, transmissions and receipt of data, calendars, directories and distribution lists, draft documents, and all other forms of electronic communications.

Except as provided for in Section 6 of this directive, use of the City's electronic communications system shall be restricted to the performance of matters which relate to official functions of the City of Detroit government. These matters include all activities which concern the operation of City government, and the delivery of governmental services to the public. This directive provides guidelines for authorized users to ensure proper and effective use of the system. Further, this directive establishes a policy for the protection of one of the City's most valuable assets: information.

2. Authorized Users

All City department and agency employees, in-house contractors, independent contractors, interns, students, volunteers, and all other persons having authorized access to City systems shall be considered authorized users of the City's electronic communications system and, therefore, are subject to this directive. However, the City retains the right to cancel, restrict, or otherwise change an authorized user's access to the City's electronic communications system.

3. City Property

It is the policy of the City that any electronic communication created, received, transmitted, or stored through use of any part of the City's electronic communications system including, but not limited to, all hardware and software, is the property of the City. Accordingly, any electronic communication created, received, transmitted, or stored in the City's electronic communications system is not considered, in whole or in part, as private in nature regardless of the level of security on the communication. Further, in accordance with the applicable

law governing access or disclosure, the City reserves the right to access electronic communications under certain circumstances and/or to disclose the contents of the communication without the consent of the authorized user who created, received, transmitted, or stored the communication.

4. Public Records

While the City's electronic communications system provides its authorized users with a convenient and efficient means of communication, this resource must be consistently managed with due regard for the applicable law governing the creation, receipt, retention, use, and disclosure of public records. Generally, a public record means information created, owned, and used in the possession of, or otherwise retained by, a public body in the performance of an official function, from the time it is created. See the Michigan Freedom of Information Act (FOIA), being MCL 15.231 et seq; MSA 4 1801(1) et seq. Since electronic communications are often deemed under the law to be public records, all authorized users are put on notice the law provides that, in certain instances, electronic communications transmitted, or stored, via any electronic system are subject to disclosure and litigation. Therefore, authorized users of the City's electronic communications system must bear in mind that, whenever creating and sending an electronic communication, they are almost always creating a public record which is subject to disclosure whether the communication is routine or intended to be confidential. Further, a recent amendment to the Michigan FOIA provides that a "written request" for a public record means a writing that asks for information, and includes a writing transmitted by e-mail or other electronic means. Thus, authorized users who receive any electronic communication from a non-City person who, or entity which, requests information from the City shall immediately forward the request to the Law Department for an appropriate response.

5. Security

The Information Technology Services (ITS) Department is responsible for the development, implementation, maintenance, and enforcement of security procedures to ensure the integrity of the City's electronic communications system, regardless of the medium. This includes, but is not limited to a centralized enterprise-wide security scheme that uses identification authentication programs, access logs, and audit trails; transmission procedures, firewall, and encryption technology; C2 security standards; back up procedures and schedules; controlled software configurations; access administration; individual passwords; and hardware theft protection. Authorized user passwords shall be required to access the City's electronic communications system, and software shall be programmed to change all user passwords periodically. All authorized users are responsible for exercising due care in maintaining the secrecy of their individual password, and in monitoring the use of their individual workstation.

6. Acceptable Usage

The use of electronic communication is encouraged when such use is the most cost-effective and/or efficient means of communication. However, use of the City's electronic communications system shall avoid interference with the work of other authorized users, and disruption of any network services or stored data. The use of electronic communications shall be governed by the same policies and guidelines that govern the use of any other type of City resource. Therefore, the City's electronic communications system shall be used in an honest, ethical, and legal manner which follows applicable licenses, contracts, and policies according to their intended use. Authorized users are responsible for being aware of available information resources, and that these resources are being shared. Authorized users shall refrain

from all acts which waste, or prevent, other authorized users from utilizing available City resources.

Use of the City's electronic communications system by any authorized user for advertising, for commercial use, or for solicitation, in any form or format is prohibited. In accordance with the applicable law and consistent with efficient government, practicality, and this directive, department directors, agency heads, members of boards, and commissions, City Council members, and the City Clerk, or their designees, shall be responsible for defining and monitoring the use of the City's electronic communications system for matters not in the performance of an official City function.

Authorized users are prohibited from using the City's access to the Internet for matters not related to any official City function, including personal searches and personal Internet e-mail messages. However, authorized users may use Intranet e-mail for communications that are incidental to the performance of an official City function, such as notifying other authorized users of an employee's illness. Authorized users should bear in mind that internal, or external, audits may be used to examine the City's access to the Internet and, where appropriate, the City may block access to discourage use of the Internet that is inconsistent with this directive. ✓

Electronic communications that may result in the loss of an authorized user's work product, or in damage to the City's electronic communications system, are prohibited. Any attempt to willfully tamper with, or damage, any file or communication is prohibited. Electronic communications sent by misrepresentation, or attempted concealment of identity, are prohibited. Any usage done under the access code of an authorized user is the responsibility of that individual. Authorized users are responsible for protecting their access authorization, and shall take all reasonable precautions to protect files, messages, passwords, and unauthorized access and use of the City's electronic communications system including, but not limited to, logging off a workstation when appropriate to prevent unauthorized use of the system.

Authorized users of the City's electronic communications systems are warned that dangerous and unethical software exists which can introduce viruses into the system, break passwords, and observe mail packets. Although it is the City's intent to detect and eradicate this type of software and/or infected data, authorized users are advised to use appropriate precautions when using programs, or data from a source outside one's own department or agency, including downloading software programs and data from the Internet. Authorized users must also bear in mind that downloading programs and files from the Internet may violate federal copyright law.

7. Appropriate Content

The workforce for the City is a diverse population, which holds divergent opinions. However, the City's electronic communications system shall not be used to transmit any communication that contains statements, or material, of a derogatory nature toward any specified person, or toward any race, nationality, gender, marital status, sexual orientation, religion, disability or physical characteristic, or age group. Any language or statements that are made on, or acts made via, the City's electronic communications system which could be construed as defamatory, discriminatory, or harassing, are prohibited. All guidelines and prohibitions that are contained in federal, state, and City laws and which govern the protection of civil rights shall be strictly enforced. The City's electronic communications system shall not be used for proselytizing, or for promoting any religious belief or tenet, or for campaigning for,

or against, any ballot proposal, or any political candidate or issue.

8. Privacy and Inspections

Because all electronic communications are the sole property of the City, an authorized user may assume a 'rule of thumb' that any electronic communication created, received, transmitted, or stored on the City's electronic communications system is public information, and may be read by anyone. All authorized users of the City's electronic communications systems are made aware that once an electronic communication is sent, the sender probably cannot delete or retrieve the message. Further, software programs allow backup copies to be made of all electronic communications on the system, including communications believed to be 'deleted' by the authorized user. Any item created, received, transmitted, or stored on the City's electronic communications system is not considered to be a personal or a private communication of any authorized user.

Electronic communications may be intercepted, forwarded, destroyed, stolen, or read like a postcard over an open network. Therefore, authorized users are prohibited from electronically transmitting confidential or sensitive information via inter, or intra, network services unless it is encrypted.

City technicians, and other authorized persons, may inspect programs, files, documents, or any other data on the City's electronic communications system for routine system maintenance, repairs, updating or monitoring activities. City technicians, and other persons, who are authorized to maintain, repair, update, or monitor activities shall respect the rights of authorized users. Therefore, such persons shall not intentionally seek information on, obtain copies of, or modify files, documents, or other data that may be confidential or not open to public inspection or release. Further, authorized users must be aware that technicians, and other authorized persons, may utilize software to legally assist the City in monitoring time accounting and work content, and in determining error rates.

9. Supplemental Policies or Guidelines

Department directors, agency heads, members of boards and commissions, City Council members, and the City Clerk, or their designees, are responsible for the execution of, and adherence to, this directive. Because departments, agencies, boards, commissions, City Council members, and the City Clerk have unique responsibilities or duties, there may be a need to adopt and administer supplemental policies and guidelines regarding the use of the City's electronic communications system. Any supplemental policies or guidelines implemented by any department director, agency head, board, commission, City Council member, and the City Clerk shall not relax, or conflict with, any policy or guideline contained within this directive.

10. Acknowledgment

To ensure compliance with the City's policy and guidelines governing use of the City's electronic communications system, all authorized users of the City's electronic communications system are responsible for being familiar with this directive. As such, department directors, agency heads, members of boards and commissions, City Council members, and the City Clerk shall ensure that each authorized user receives a copy of this directive, and signs and dates a copy of the attached acknowledgment. The completed acknowledgment shall be maintained in the authorized user's file.

11. Compliance Required

Department directors, agency heads, members of boards and commissions, City Council members, and the City Clerk, or their designees, shall be responsible for ensuring that authorized users remain in compliance with this directive. This includes: reporting any information which concerns either a bypass of this directive, or a security issue regarding the City's electronic communications system; investigating noncompliance with this directive; and implementing necessary disciplinary, or corrective, action when the City's electronic communications system is used contrary to this directive.

Where information is received concerning possible noncompliance with this directive, the department director, agency head, members of boards or commissions, City Council members, or the City Clerk, or their designees, shall document and investigate the instance in accordance with departmental or agency rules, and with the City Civil Service Rules. Where appropriate, the City may institute internal discipline and/or civil or criminal action.

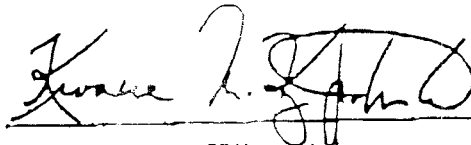
The City reserves the right to cancel an authorized user's access to the City's electronic communications system for noncompliance with this directive. The City may withdraw an authorized user's password and access without notice.

12. Purge and Archival Schedules

The purging and archiving of electronic communications which are created, and used, in the performance of an official function shall be consistent with approved public record retention and disposal schedules. In conjunction with ITS, department directors, agency heads, members of boards and commissions, City Council members, and the City Clerk shall ensure that all software is programmed to comply with approved retention and disposal schedules.

13. Effective Date

This directive is effective on April 6, 1998.



Kwame M. Kilpatrick
Mayor