CITY OF DULUTH

Human Resources Manual

CHAPTER: 60 – TECHNOLOGY POLICY

EFFECTIVE DATE: 01-01-2009; updated 05-01-2012

Note: This Technology Policy was originally issued on 3-22-2005 as a stand-alone policy. The original policy has been renumbered and reformatted to fit the design of the Human Resources Manual.

60.01 PURPOSE & POLICY

A. Technology is Provided for the Benefit of the City

Technology is a valuable and costly city resource provided to city employees for the benefit of the City's business. Irresponsible or unauthorized use of technology resources reduces their availability for critical business operations, compromises network security and poses other risks to the City's efficient and professional operation.

B. Policy

This purpose of this policy is to instruct employees on their duties and responsibilities with regard to technology provided by the City and to define authorized uses and prohibited uses of such technology.

60.02 DEFINITIONS

1. Archive - To copy files into a long-term storage medium in order to retain for utilization backup.

2. Copyright Infringement - "Copyright" is the exclusive right of a person or a legal entity to reproduce, publish or sell a work (e.g., a picture, written article or a computer program) which it has created. Copyright infringement may occur if, for example, an individual copies a computer program or other work without the author's permission. E-mail messages which have computer programs or artwork attached to them should be carefully analyzed to insure that no copyrights are violated by the use or other reproduction of the program or artwork.

3. Distribution List - A list of intended recipients of an e-mail communication.

4. Electronic Mail ("e-mail") - Communications within and among Microsoft Exchange, the City of Duluth Home Page, Mindspring, Windows Internet Mail, Microsoft

Internet Explorer, etc.

5. E-mail Records Master Copy - The archived e-mail records maintained by the City.

6. Encryption - The translation of data into a secret code.

7. Inspect - The entire range of actions by the City in order to control its technology users and usage, including, but not limited to: monitoring, interception, audit, review, inspection, copying, disclosure, and retrieval.

8. LAN - "LAN" is the acronym for Local Area Network .A network (or group) of personal computers and related devices (e.g., printers) in a small area (such as an office) that are linked together by cable; that can directly communicate with other devices in the network; and that can share resources (e.g., directories and files). LAN Administrators are those individual(s) in charge of insuring that the LAN works properly.

9. Network Server - A computer which is dedicated to managing network traffic. Individual desktop computers rely on network servers for files, printers and software.

10. Technology - All forms of internet access, electronic mail ("e-mail"), voice mail, computer equipment, computer software, telephones, cell phones, radios, pagers, and other similar devices or functions

11. WAN - "WAN" is the acronym for Wide Area Network, which is a network (or group) of LAN's.

60.03 NO CONFIDENTIALITY OR EXPECTION OF PRIVACY; OWNERSHIP

A. All employees are hereby notified that there is no confidentiality, nor expectation of privacy in the use of any technology provided by the City. This includes, but is not limited to: all information transmitted, generated, received, or stored on the City's computer system, or any information processed, generated, received or transmitted by the use of telephones, cell phones, radios, pagers, copy machine, fax machine, or any other similar device or function. This includes both the use of the City's technology for official business use and for authorized personal use.

B. Information, messages and/or documents processed, transmitted, generated or received in any way by the use of City technology are City property and may be retrieved from storage even though they have been deleted by the sender and receiver. These messages may be used in disciplinary proceedings.

C. Employees are cautioned that any message sent electronically can be intercepted, read, stored, or re-transmitted outside the City's control and, as such, there should never be an expectation of privacy.

D. Electronic messages can never be unconditionally and unequivocally deleted. The possibility of discovery always exists. Use caution and judgment in determining whether a message should be delivered in person instead of electronically.

E. Employees should be aware that if they use the technology to transmit personal messages, such messages will be treated no differently than other transmissions and

may be accessed, reviewed, copied, deleted, or disclosed by the City. Employees should not expect that a personal message will never be disclosed to or read by someone other than the intended recipient(s).

F. The use of computer passwords or account codes do not ensure or suggest any confidentiality or expectation of privacy. Electronic messages are not the private property of the sender or recipient, even though passwords or encryption codes are used for security reasons.

G. Employees are reminded that anytime they use the City's network or Internet connection, that connection is traceable to the source. Employees are reminded that this City's Internet Protocol (IP) address is transmitted to, and can be traced by, Internet sites visited.

H. The City's technology is City property. All communications, by whatever form or nature, conducted over City property belong to the City, and not to the employee.

60.04 INSPECTION BY THE CITY

A. All information transmitted, generated, composed, received, or stored on the City's computer system, or in any message transmitted by the use of any City technology is subject to inspection at any time without prior warning or notice to any employee and without the knowledge of any employee. Such actions may be conducted using content filtering software, or by designated City employees, and/or designated external entities.

B. The City has the capability and authority to evaluate the performance and use of its technology resources, and will routinely monitor their use. Some of the concerns of the City include cost analysis, security, bandwidth allocation and the general management of the City's gateway to the Internet.

C. The City reserves the right to alter, modify, re-route, or block the delivery of messages or content as appropriate. This includes, but is not limited to:

1. Rejecting, quarantining or removing the attachments and/or malicious code from messages that may pose a threat to City technology resources

2. Discarding attachments considered to be of little business value and of significant resource cost

3. Rejecting or quarantining messages with suspicious content or containing offensive content

4. Re-routing messages with suspicious content to designated City employees for manual review

5. Rejecting or quarantining messages determined to be unsolicited commercial e-mail (spam)

D. Department Heads/Supervisors have the authority to inspect the contents of any equipment, files, calendars or electronic messages of their subordinates in the normal course of their supervisory responsibilities. The Management Information Systems

Coordinator, or other authorized personnel shall extract stored messages when requested to do so by authorized City personnel.

60.05 PROHIBITED ACTIVITIES

The following activities are prohibited at all times, while using any of the City's technology in any manner:

1. Using technology to conduct any type of illegal activity.

2. To violate, attempt to violate, or conspire to violate any federal law or regulation; state law or regulation; City ordinance, resolution, directive, policy, procedure, or rule; or any other external directive to which the City is bound (i.e., criminal history rules of GCIC)

3. Accessing, disseminating, or storing any adult pornographic material(s), links to websites, or anything which could be construed as sexually explicit , scandalous, defamatory, libelous, illegal, immoral or unethical (including hate, illegally discriminatory, or racist literature or messages)

4. Sending or posting threatening, defamatory, slanderous, racially and/or sexually harassing messages, remarks, or proposals; including the use of vulgar or obscene language

5. Composing or sending any message which contains racial or sexual slurs or jokes, or otherwise contains patently harassing, intimidating, abusive or offense material (pictures, images, words, etc.) to or about others

6. Use of technology to harass or discriminate against an individual(s) on the basis of sex, age, race, national origin, religion, disability, sexual preference, political belief, and any other characteristic or status protected by federal, state or local law

7. Using the technology to harass, stalk or annoy another person, such as the persistent annoyance of another user or the interference in another user's work, (e.g. the sending of unwanted e-mail)

8. Using the technology to intimidate, coerce, or antagonize another

9. Using for commercial, promotional, or business purpose for financial gain (e.g., transmitting personal messages offering to buy or sell goods or services, or operating a business)

10. Advertising, trading, giving away, soliciting, or providing goods or services (except under specifically authorized circumstances and conditions, such as HR sponsored employee morale, or discount programs, or Credit Union-sanctioned activities)

11. Using City technology to conduct any unauthorized employee organization or association business

12. Promoting, conducting, or soliciting for political campaigns or activities

13. Intercepting, eavesdropping, recording, altering, deleting, examining, copying, or

modifying another employee's electronic messages without consent of the other employee

14. Forward an electronic message to another without the permission of the originator, unless the message is not confidential and forwarding of the message is clearly in the interest of the City

15. Sending, attempting to send, transmitting, or re-transmitting, anonymous messages

16. Adopting the identity of another person or misrepresenting yourself as someone else or in any way being deceptive as to the true identity of the sender

17. Propagating a computer worm or virus, or any other program or material which may have a debilitating or disabling affect on the City's technology; or performing any unauthorized, deliberate action that damages or disrupts technology, alters its normal performance, or causes it to malfunction

18. Sending or receiving messages (including software) in violation of copyright law.

19. Sending or receiving software in violation of software licensing agreements

20. Improper distribution, revealing or publicizing proprietary, confidential or privileged information

21. Attempting to override, disable, tamper with, or avoid any security or integrity procedure, measure, or device

22. Attempting to tamper with or inappropriately access ("break into") any technology of the City, or of another organization or person

23. Subscribing to mail lists or list servers that are not related to official City business, or to professional enhancement/development in support of the City's business

24. Participating during duty hours in unauthorized chat rooms, which are not related to City business or to job related/professional development

25. Playing computer games during duty hours

26. Use of technology for gambling

27. Use of technology to conduct union business or activities

28. To promote/defame religious perspectives

29. Establishing personal web sites or bulletin board systems

30. Using the City Seal, Departmental logos, or other similar markings to misrepresent personal materials as falling under official City auspices

31. Intentionally misrepresenting, either implicitly or explicitly, personal views or comments in electronic forums or e-mail as official City of Duluth policy or position (If there is a reasonable expectation that a personal communication could be

interpreted as official business, then a disclaimer shall be used. For example: "My personal opinion is….", or "while not speaking on behalf of the City, I think that….") Any and all opinions communicated using any technology, whether express or implied, are those of the individual and do not necessarily express the opinions of the City or its administration and elected officials.

32. Malicious attempts to harm or destroy data of another user, the Internet, this or other networks

33. Sending messages or providing information that could damage the City's reputation

34. Sending messages that are deliberately misleading or deceptive

35. Searching for outside employment, except while employee is on their own time

36. Using any inappropriate background screen images (e.g., screen savers, etc.)

37. Downloading screen-savers and/or games from the Internet

38. Downloading audio and/or video clips from the Internet, unless it is specifically related to the employee's job duties

39. Viewing or posting of messages, replies, or any type of announcements to the Internet via message boards, forums, chat rooms, on-line classified, news groups, list serves, or any other type of public web site, unless directly related to the employee's job duties and not in conflict with any other part of this policy

40. Use of computer systems and/or networks in attempts to gain unauthorized access to other computer systems ("remote systems")

41. Decryption of system or user passwords

42. Copying of system files

43. Attempts to secure a higher level of privilege on network systems than authorized

44. Downloading of files from peer-to-peer networks (e.g., Kazaa, etc.)

45. Downloading files or attachments from outside e-mail services (AOL, MSN, etc.)

46. Subscribing to push technology services that are not related to official City business or to professional enhancement. This refers to subscription type services that send information to personal computers automatically and routinely as a result of prior registration by the user. Examples of such services include: weather reports, sports news, hobby updates. Permitted push technology services are those that provide information on City business or professional enhancement topics, such as Government, environmental, health, or technology related subjects. E-mail alerts are permitted (such as for severe weather, breaking local news, etc.).

47. Entering into any lease or contract for professional services that relates to computer hardware and/or software (this includes design, support or maintenance of computer hardware/software, networking, Internet, and computer repair services)

48. Changing system settings (network neighborhood, device setup, Internet access options, system registry, control panel Regional Settings, or any other areas dealing with advanced settings which may alter your computer's performance, etc.), except for printer's properties

49. Move or change ANYTHING in any computer server room

60.06 INADVERTENT ACCESS; RECEIPT OF INAPPROPRIATE MATERIALS

A. Inadvertent Access

1. It is important to distinguish between passive or inadvertent receipt of materials, on the one hand, and actions which require deliberate decision, on the other.

2. For example, it is possible for an employee to:

- Be sent unsolicited sexually-explicit or racist materials; or
- Be misled by a search engine's links, such as to accidentally open offensive materials.
- Misdial a phone number

3. Such activities should be distinguished from those of an employee who consciously accesses, downloads or distributes sexually-explicit materials.

4. Employees who inadvertently access an adult pornographic or other prohibited website or telephonic location shall report this to their supervisor immediately. Inadvertent access shall be treated as a mistake.

B. Receipt of Inappropriate Materials

If an employee receives inappropriate/prohibited material from another person, they will immediately advise the sender that they are not permitted to receive such information and not to send similar material again. If the employee needs assistance in responding to such situations, they will contact their supervisor who can assist them or arrange for assistance from other city employees (e.g., if the other party does not cooperate, contact the Information Technology department for guidance in blocking transmissions from the offending party.)

60.07 CONFIDENTIAL, PRIVILEGED OR COPYRIGHTED INFORMATION

A. Confidential Information

1. Georgia law requires that all employees protect the integrity of any confidential information generated by or on behalf of the City as well as confidential information concerning others.

2. Employees must exercise a greater degree of caution in transmitting confidential information through technology than with other modes of communication because of the ease and simplicity with which this information can be redistributed. Confidential information should never be transmitted or forwarded to persons who do not have a "need to know" the information.

3. To reduce the chance that confidential information may inadvertently be sent to the wrong person, ensure that any distribution lists used are current prior to the transmission of information. Review each name on any list of recipients before transmission to ensure that all recipients have a need to know the information.

4. City employees should consult the appropriate Department Head, Supervisor, or, if necessary and authorized, legal counsel to answer any questions regarding the confidentiality of information.

5. Types of information often considered confidential include, but are not limited to, the following:

    a. information from an individual's personnel file

    b. personal information about employees, such as home addresses and phone numbers

    c. information relating to potential litigation, existing litigation, claims against the City, administrative hearings of a criminal or civil nature, or any judicial proceeding

    d. information which, if released, would give a competitive advantage to one competitor or bidder over another

    e. a draft or working paper involved in the preparation of proposed legislation

    f. private correspondence of elected officials

    g. trade secrets

    h. commercial or financial information of outside businesses

    i. information related to the regulation of financial institutions or securities

    j. social security numbers

    k. personal/family information of City employees

    l. photographs of peace officers

    m. certain information the City obtains from businesses pertaining to environmental audits.

6. Messages that contain confidential information should have a confidentiality legend in all capital letters at the top of the message in a form similar to the following: "THIS MESSAGE CONTAINS CONFIDENTIAL INFORMATION

OF THE CITY OF DULUTH. UNAUTHORIZED USE OR DISCLOSURE IS PROHIBITED."

An additional message can be used (such as on a fax cover sheet, or at the end of the communication) in a form similar to the following:

"This communication and any files transmitted with it, is intended solely for the individual or entity to which it is addressed and may contain confidential, private, and/or privileged material. Any review, retransmission, dissemination or other use of or taking action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you are not the intended recipient, or believe that you have received this communication in error, do not print, copy, retransmit, disseminate, or otherwise use the information. You should reply to the sender and indicate to the sender that you have received this communication in error, and then delete this communication and any accompanying files you received. Thank you."

7. Since copies of messages (particularly e-mail) may be placed on back-up or other systems out of the control of the City employee generating the message and/or may be accessed by information system personnel or others who do not need to know the information, all employees should remember that it may be inappropriate to communicate certain types of confidential information through the e-mail system.

8. In addition, to minimize the inadvertent disclosure of confidential information, employees should not access their e-mail messages in the presence of others unless such messages have been reviewed to ensure that the information contained therein is not confidential. Messages should not remain visible on the monitor when a user is away from his or her computer.

9. Caution should be used when transmitting confidential information. Any employee who knows or suspects that confidential information has been compromised is to report this to their immediate supervisor as soon as possible.

B. Attorney-Client Privilege

1. All messages to and from the City Attorney or other legal counsel seeking or providing legal advice or otherwise pertaining to pending or potential litigation, settlement, claims, administrative proceedings, or other judicial actions are legally privileged information and should be marked with the following legend in all capital letters at the top of the message:
"CONFIDENTIAL ATTORNEY/CLIENT PRIVILEGED INFORMATION"

2. In addition, in order to preserve the attorney-client privilege, messages to and from the City Attorney should never be sent to others via distribution lists, should never be forwarded to anyone else, and should never be retained on a network e-mail system. If it is necessary to retain a copy of an attorney-client privileged communication, it should be printed and placed in the appropriate file. Confidential communications between the City and its legal counsel should not be archived for disclosure to the public.

C. Copyright Infringement

The ability to attach a document to a message for distribution to others greatly enhances the risk of copyright infringement. A system user can be liable for the unauthorized copying and distribution of copyrighted material through technology. Accordingly, City employees should not copy, retrieve, modify, distribute, or forward copyrighted material of a third party (such as software, database files, documentation, articles, graphics files and down-loaded information) without advance confirmation that the City has the right to copy or distribute such material. Any questions concerning copyrighted information should be directed to the City Manager or, if necessary, the City Attorney.

60.08 INTERNET ACCESS

A. Site searching and access is limited to those sites that provide useful information to City business. The access to the Internet is provided to employees for bonafide job duty use only and for authorized personal use. Internet access is a privilege, not a right. Employees are not authorized to utilize the City's Internet access for any unauthorized use.

B. The City reserves the right to monitor web sites visited by employees using City technology. The City may use software to undertake such monitoring or may use other methods of inspection and surveillance to ascertain employee internet use.

60.09 ELECTRONIC MAIL ("E-MAIL")

A. Personal E-Mail

Personal e-mail shall be defined as email that is not part of the Duluth e-mail system that is accessed through the Internet or third party programs such as America On Line or Microsoft Network.

If an employee uses any computer or appliance from inside the Duluth computer network to view personal e-mail over the Internet, they may not, under any circumstance, download or activate any attachments to e-mails. Exceptions may be made by the IT department only

If a computer or appliance owned by the City of Duluth is used to view or send personal e-mail, there should be no expectation of privacy with respect to such e-mail just as there is no expectation of privacy with any e-mail

B. E-Mail Contact Between Employees and Mayor/Councilmembers

Only Department Heads (and their designees) should send e-mail to the Mayor and Councilmembers A copy of all communication between employees and Council/Mayor must be sent to the City Clerk. Likewise, the Mayor and Councilmembers should not send e-mail directly to employees, but should direct them through the appropriate Department Head, and a copy of all such e-mails must be sent to the City Clerk.

60.10 SEPARATION FROM EMPLOYMENT

Upon separation from the City's employment, the City will deny all access to technology

resources, including the ability to download, forward, print or retrieve any messages stored in the computer system, regardless of sender or recipient.

60.11 DISCIPLINARY AND/OR LEGAL ACTION

A. Violations

Violations of this policy will be evaluated on a case-by-case basis and may result in:

- restriction, suspension or loss of technology access or capability, and/or
- disciplinary action up to and including termination.

B. Violation of Other City Policies

Some violations of this policy (such as sending sexual or discriminatory messages) may also constitute violations of other City policies (such as the policy prohibiting sexual harassment or discrimination).

C. Violation of Federal or State Law, or Administrative Regulations

Some actions involving the use of technology may also violate federal or state law. Violations of this policy or misuse of City technology which are of a criminal nature may be referred to the appropriate authorities for criminal prosecution.

Some actions involving the use of technology may also violate federal or state regulations (such as the GCIC regulations regarding criminal history record information). The City may be sanctioned for such violations, and the individual(s) responsible for the violation may be disciplined.

60.12 OFFICIAL ISSUANCE OF POLICY

By our signatures below, we do hereby declare this policy to be in effect as an official policy of the City of Duluth.

Police Department SOP 05-01 “Internet Access, E-Mail, Voice Mail & U.S. Mail”, except for section 05-01-08 on “U.S. Mail” is hereby superseded by this city-wide policy.

/s/ Phil McLemore
Phil McLemore, City Manager

/s/ Teresa Lynn
Teresa Lynn, City Clerk

/s/ Randy Belcher
Randy Belcher, Chief of Police

60.98 REFERENCES

A. City of Ontario v. Quon, 130 S. Ct. 1011 – U.S. Supreme Court 2010

B. The basis for an employer's right to monitor electronic information is The Electronic Communications Act of 1986 (18 U.S.C. Section

2510, etseq). The ECPA provides for employer monitoring of electronic communication if the device monitored is used in the normal course of business. The device should be owned by the employer and be part of the business network.

60.99 UPDATES TO THIS POLICY

A. Section 60.98 "References" added with the City of Ontario v. Quon and the ECPA added (5-1-2012)

B. "City Administrator" changed to "City Manager" throughout the policy (5-1-2012)