

Policy No. 755
Date: February 2, 1998
Revised: May 12, 2003
Revised: October 8, 2009

Technology Resource Use Policy

I. Purpose, Values and Outcomes

The citizens of Lynnwood expect City employees to use the City's technological resources efficiently and appropriately. This policy establishes guidelines for the use of computer applications, technology, equipment and electronic data while conducting City business. Policy compliance will ensure technology resources are used in accordance with the public trust.

II. Policy

- A) Technology Resources shall be used to conduct City business.
- B) Department Directors with assistance from Information Services are responsible to enforce this policy and monitor compliance of their personnel.
- C) On occasion an employee may be directed to operate outside of this policy to conduct research or investigations in support of City business.
- D) Infractions may subject an employee to disciplinary action up to and including termination.
- E) This policy shall apply to all City employees, council members, contractors, volunteers and others required to carry out City business.
- F) Information Services and Human Resources jointly manage the policy and procedures.
- G) Acquisitions of Technology Resource must be approved in advance by Information Services and be purchased under the rules and regulations outlined under the City Purchasing Policies.
- H) An employee is required to protect electronic data from unauthorized access by following applicable City security measures.

III. Technology Resources

Technology Resources include the following:

- Desktop personal computers, monitors, laptops, Mobile Data Computers, Tablet personal computers, printers, Multi Function Printer/Fax machines, scanners, phones, cell phones, copiers, personal digital assistant (PDA.), USB "thumb drives", portable storage devices, etc. Technology resources also include the City's network infrastructure, servers, switches, routers, network cabling, storage and backup appliances.

- Application software including MS office suite, Email, Vendor supplied and internally developed programs, etc.
- As used in this policy, "data" means information that is generated by City personnel or as a result of research activities and recorded in any tangible or electronic medium, including without limitation notebooks and worksheets, memoranda, notes, protocols, computer databases, computer images, e-mail, files, spreadsheets, web pages and all other records.
- Voice data is defined as any voice communications that travel over or is stored on the City's network and conforms to the standard definition of data.

IV. Rules

A. Internet/Intranet:

Use of the Internet, as with use of all technology resources, should conform to all City policies. Visiting "adult" or sexually oriented web sites, or sites associated with violence, hate, discrimination or other inappropriate content that creates discomfort in the workplace and have no legitimate business value is prohibited unless for work related purposes. Law enforcement efforts utilizing these sites for investigative purposes are considered acceptable but are subject to existing Lynnwood Police Department policies. If a particular use of the Internet might be considered questionable, employees should check with their supervisor before proceeding. The City blocks access to most inappropriate web sites as a normal course of business. As these sites change on a regular basis, employees may stumble upon a questionable site inadvertently. If this happens employees should notify Information Services immediately to ensure the City's controls are adjusted.

The Information Services Division works aggressively to stop Internet Spam and "pop-up" advertising from reaching employee desktops. Employees who receive pop-up advertising or Spam e-mail that they believe is inappropriate should notify the Help Desk immediately.

B. Network:

Connecting and installing Technology Resources such as desktop computers, laptops, software, peripheral equipment, USB keys, thumb drives, wireless devices, etc. to the City network must be coordinated and set up by Information Services. Personal devices** may not be loaded or attached to City network without previous approval from the Assistant Finance Director for Information Services and are only approved in rare or emergency situations. Under no circumstances are employees to load personal software onto a City computer, laptop, PDA, cell phone or Smart Phone. Use of the City network to download large business files greater than 50 megabytes will impact City

large business files greater than 50 megabytes will impact City services therefore employees must exercise caution. If employees have a need for downloading files of this magnitude, they must contact Information Services for assistance. Employees, who need to send large files, should also contact Information Services for help.

The distribution of copyrighted, patented or other information that may qualify as Intellectual Property in electronic form is prohibited and governed by Federal Law. Federal and State privacy rules govern the use of electronic information.

**Personal devices include the use of portable USB storage devices. The implementation and use of these devices needs to be approved by Information Services prior to usage. Although a valuable tool for transporting large files, they do present a substantial risk for viruses, Trojans, worms or other unstable software. Information Services will check such devices to assure that they meet specific standards.

C. Security

Due to the nature of the information stored on the City's network, security is an important aspect of our management. Several new information security standards have been established to insure protection of the data that the City accesses and manages. These security standards require that certain adjustments be made to our network access policies.

1. Password Security

Network passwords must be changed every 90 days. Employees will receive reminder notices regarding the expiration of their passwords for approximately two weeks. Employees who fail to change their passwords within the two-week time period will no longer be able to use their passwords and must call the Help Desk for assistance.

2. Background Checks

Users of specialized or highly secure systems such as staff who accept credit cards for payment or for law enforcement personnel who access the Central Justice Information System (CJIS) will be required to complete a fingerprint and background check. Since Information Services Personnel maintain all systems within the City, all Information Services personnel will be required to complete a background and fingerprint check every five years. In addition, other employees requiring

unescorted access to the Police Department will be required to complete background and fingerprint checks as required by the State of Washington.

D. User Accounts:

Each user is responsible for establishing and maintaining passwords. Each user is responsible for logging off their computer or locking their network account when leaving their computer unattended.

E. Monitoring and Employee Privacy:

The City of Lynnwood owns all data that is created, stored or otherwise produced on City technology assets including desktop computers, servers, cell phones, Smart phones or other device. In accordance with State of Washington laws and regulations, the City is required to store this information under the proscribed Retention Policy (Section V: Paragraph B). The City reserves the right to inspect and monitor any and all such communications at any time. The City may conduct random and requested audits of employee accounts in order to ensure compliance with policies and requirements, to investigate suspicious activities, and to identify productivity or related issues within the City. Internet/Email/Voice Mail communications may be subject to public disclosure requests pursuant to Public Record or other legal requests.

F. Remote Access:

Employee approval for remote access will be governed by the Remote Access Use Policy (Personnel Policy and Procedure #756).

G. E-Mail:

E-mail messages must meet the same City business code of conduct as expected in any other written form of communication. Messages sent or received via e-mail are recognized as public records and must meet the same standards as if they were tangible documents. Use of the City email to send or receive large business files as defined by Information Services is prohibited unless approved in advance by the Assistant Finance Director for Information Services or his/her designee. Users must manage their e-mail in accordance with confidentiality, record retention policies and procedures as established by the State of Washington Archives office. E-mail box storage capacity is limited and storage quotas have been established. E-mail users are expected to manage their e-mail boxes appropriately. Employees who allow their mail boxes to exceed the established quota may lose or damage their e-mails. Information is available through the

Help Desk on how to archive e-mail to help manage e-mail box capacity. Temporary increases may be granted under special circumstances and must be requested through a Department Director who will forward the request to the Assistant Finance Director for Information Services or his/her designee for review.

H) Employee Personal Use of City Technology Resources:

Technology Resources may be used for occasional but limited personal needs as defined below, as long as such use does not result in additional cost, liability, or interfere with City business, system performance and complies with the City's employee ethics policy. Personal usage should generally conform to limits typically associated with personal phone calls. This policy does not attempt to address every possible situation that may arise. Etiquette and common sense should be exercised while using City technology resources.

Inappropriate use:

1. Personal use (except "occasional but limited" use as defined below) or personal business use – or any other use for personal gain;

This includes:

- a. Using city resources to solicit other employees for ventures which are not sponsored by the city (an example of a venture sponsored by the city would be the United Way campaign or the American Heart Walk), and;
- b. Distributing information about persons or organizations outside the business of the City unless approved in advance by the Mayor;
- c. Promoting religious, commercial or political causes or campaigns;
- d. Promoting union activity unless specifically approved in advance by the Mayor or as defined by collective bargaining agreement.
- e. Any employee use for non-business purposes during time for which the employee is being compensated by the city except as authorized below.
- f. Using the City's Internet connection to listen to the radio or watch videos from such web sites as You Tube, Truveo, AOL video or other viral video site unless approved in advance by the Mayor or Assistant Finance Director for Information Services for business usage. Usage of the system to view training videos or to

participate in video meetings, Go-To-My-Meetings or similar are acceptable.

2. Violating copyright, license agreements, or other contracts – or any other illegal uses;
3. Interfering with intended use of information resources;
4. Seeking to gain unauthorized access to information resources;
5. Using any Computer System or equipment under false pretenses;
6. Using the system to participate in hacking¹, phishing², phreaking³ or otherwise participate in illegal or nefarious activities;
7. Destroying, altering, dismantling or otherwise interfering with the integrity of computer based information and/or information resources without authorization;
8. Transmitting or causing to be transmitted, communications that may be construed as sexually suggestive, offensive, demeaning, insulting, harassing or disparaging of others. Messages which may be considered offensive are any messages which contain sexual implications, religious slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability;
9. "Occasional but limited" use as defined by WAC 292-110-010 is permitted. Examples of "occasional but limited use" as defined by WAC 292-110-010 include:
 - A. Use of the e-mail (or phone) during breaks to confirm that children have arrived home safely from school;
 - B. Wishing a "happy birthday" or advising of an "agency" social event over e-mail;
 - C. Advising employees of recreation center activities or opportunities;
 - d) Use of the internet to retrieve general information during non-working time (i.e. reading the newspaper on-line).

V. Public Disclosure

- A. Generally, all e-mails dealing with City business, regardless of where they are sent to or from, are considered "public records" and subject to

¹ Hacking: Unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network

² Phishing: is the act of tricking someone into giving them confidential information or tricking them into doing something that they normally wouldn't do or shouldn't do such as revealing personal financial information or Social Security numbers. Commonly used in Identity theft cases.

³ Phreaking: is the act of hacking the telecommunication(phone) systems

the Public Records Act ("PRA") and record retention laws. E-mail may also be subject to legal processes such as subpoena. Every writing relating to the conduct of government or the performance of governmental functions, whether written, recorded, taped, or electronically stored, should be considered a public record and subject to public inspection.

B. Public Records. The following are examples of types of e-mail messages that may qualify as public records:

1. Discussions regarding any city business that could be or has been discussed by the city council, including discussions with constituents, friends, family members, other council members, staff or officials of other cities, regardless of their relationship with you, and Municipal Research & Services Center (MRSC..
2. Policies and directives, including preliminary drafts, notes, recommendations, and intra-agency memorandums in which opinions are expressed or policies formulated or recommended, unless otherwise exempted, correspondence or memoranda related to official business, work schedules and assignments, agendas and minutes of meetings, drafts of documents that are circulated for comment or approval, any document that initiates, authorizes, or completes a business transaction, and final reports or recommendations.

C. Non-public records. The following are examples of types of e-mail messages that would likely not qualify as public records:

1. Personal messages and announcements not related to official business;
2. Personal email addresses, residential addresses, phone numbers, passwords;
3. Information-only copies or extracts of documents distributed for convenience of reference;
4. Published reference materials;
5. Copies of memoranda, bulletins or directions of a general information and non-continuing nature;
6. Announcements of social events, such as retirement parties or holiday celebrations;
7. Emails regarding candidates for the council or personal election strategy;
8. Unrecorded conversations.

- D. Exemptions. E-mails that qualify as public records are subject to disclosure under the Public Records Act (PRA), unless they fall under one of the specific exemptions. The most common are:
1. Preliminary drafts, notes, recommendations, and intra-agency memorandums of recommendations, opinions, and proposed policies *until* the policy is adopted; once recommendations are implemented they are no longer exempt protection from disclosure;
 2. Personal/private matters the disclosure of which would be highly offensive to a reasonable person, and are not of legitimate concern to the public;
 3. Attorney-client communications only if transmitted in confidence between an attorney and a public official or city employee acting in the performance of his or her duties for the purpose of obtaining legal advice.
 - ◆ The exemption is lost if shared with a third party, such as MRSC;
 - ◆ It does not include records merely because they reflect communications in meetings where the attorney was present or because a copy was provided to the attorney;
 - ◆ Attorney-created work product documents involving a contemplated, existing, or reasonably anticipated litigation.
- E. Policy Guidelines
1. All email concerning city business should be transmitted via city email accounts, not personal or business accounts;
 2. All personal email should be transmitted via personal email accounts, not through city email accounts;
 3. Emails subject to privilege/exemption, such as attorney-client privilege, should not be shared with third parties, or the privilege/exemption may be lost;
 4. All PRA requests should be referred to the Administrative Services Department for coordination and tracking.
 5. If a PRA request is received, it should be assumed that pertinent documents are subject to the PRA request, and copies should be provided to the city attorney for a determination of whether there is an applicable exemption.
 6. If a message is not appropriate for the newspaper, it should not be sent!

7. Employees are generally prohibited from sending messages to the ~All User e-mail. Approval for the use of ~All User is the sole domain of the Department Directors or the Mayor in consultation with the Assistant Finance Director for Information Services. *Any use of the ~All User e-mail account must be cleared through the Information Services Director's office prior to sending.*

The use of attachments to the ~All User e-mail address must also be approved in advance by the Assistant Finance Director for Information Services. Large attachments will not be allowed. Information Services staff will work with the sender to provide a different, less network intensive method of delivering information wherever possible.

F. Record Retention

In addition, all e-mails that qualify as public records must be retained in accordance with record retention laws (See Public Records Act Policy #2006-003).

Record retention laws are applied based on the content rather than the form (i.e. e-mail); e-mail records must be classified within the appropriate record retention schedule. For instance, the e-mail itself may be considered correspondence, but may include attachments such as reports, contracts, or accounting records that fall under other specific retention schedules. The following guidelines should be followed for records retention of e-mail.

G. E-mail Retention Requirements

All e-mail messages must be stored electronically. Information Services staff will provide guidelines for electronic storage. Employees must follow those guidelines to ensure that the City's technological resources run efficiently.

VI. Responsibilities:

Supervisors:

- Supervisors shall be responsible for assuring their employees understand and comply with the policy.

Employees:

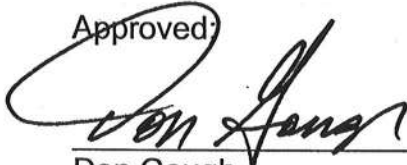
- Employees are responsible for understanding and complying with the policy and will be subject to disciplinary action up to termination depending on the infraction of the policy.

- If the activities of an employee are found to violate City policy or law the employee will assume all expenses related to resolving the matter and will not be represented by the City.

Directors:

- Directors are responsible for the oversight and appropriate use of the Technology Resources.
- Each department director is responsible to enforce this policy in consultation with the Human Resources Director and the Mayor.

Approved:



Don Gough

9-28-09

Date

Technology Resource Use Policy

Employee Acknowledgement Form

I recognize and understand that the City's Technology Resources are to be used in a manner consistent with conducting City business as described by the policy and I understand that I will be subject to disciplinary action up to termination depending on the infraction.

As an employee of the City of Lynnwood, I have read and understand the City's policy on Technology Resources Use Policy (dated October 8, 2009).

Printed Name

Signature of Employee:

Date

Signature of Supervisor:

Date