LEAGUE OF MINNESOTA CITIES

CONNECTING & INNOVATING
SINCE 1913

RISK MANAGEMENT INFORMATION

DEVELOPING A COMPUTER USE POLICY

An effective computer use policy takes a comprehensive look at employee use of a city's technology, identifies when and how city technology can be used, and identifies precautions cities should take. Ideally, the policy is developed in consultation with technology and human resources experts.

Key Components to a Computer Use Policy

An effective computer use policy governs when and how employees use city-provided technology resources, appropriate and allowable use of city managed e-mail, electronic communications, social media and Internet access, what sorts of precautions they should take against things like computer viruses, and what could happen if they break the policy.

A good computer use policy can help:

- Ensure city staff understand technology dangers.
- Protect city technology and data assets.
- Increase employee productivity by not having to clean up things like virus outbreaks and junk e-mails.
- Help employees avoid inappropriate information exchanges through electronic communications such as social media.
- Prevent liability if your city's computer system infects someone else's or your confidential files are breached.

Ideally, a computer use policy should be developed in consultation with technology and human resources experts. Technology considerations might include issues of managing equipment, access and protection of the city's computer network and data. Human resources might have input regarding allowable personal use of city resources and ramifications of inappropriate employee computer use.

There are many areas in a computer use policy that cross boundaries between technology and human resources policies. As you think about an appropriate computer use policy for your city, you might weigh some of the following considerations.

Be realistic

It may be impractical to forbid personal use of the city's computer. Employees are unlikely to follow this and you might not be able to monitor or enforce the policy. Try to strike a balance between the need for security and cumbersome rules.

Balance technology and performance issues

It might be tempting to try solving a performance issue like an employee who spends too much time surfing the Internet by implementing a technology policy against personal use of the city's Internet connection. Make sure your computer use policy is about computers and use other policies to address employee performance.

Focus on education

Most employees won't deliberately introduce viruses or other nasty stuff into the city's computer system, but the majority of folks might not understand how visiting a website for music lyrics can be dangerous to the network. Explain it to them and they'll be more likely to follow procedures. Think about frequent communications and updates as a way to remind folks about the policy you've put in place.

Keep it simple

A computer use policy should be specific, and include easy-to-understand guidelines and examples. Think about when to roll something into your existing policy and when to create a new policy; such as whether you include rules about city-owned cell phones in a computer use policy or create a stand-alone policy for phone use.

Learn More

Read more about risks related to electronic communications between council members, social media and cities, and more in the following materials from the League:

Electronic Communications Between Council Members

Social Media and Cities: Questions and Considerations

Managing Your City's Electronic Records

Complying with the Minnesota Government Data Practices Act

These items and more are at in the Resource Library of http://www.lmc.org

Supplement the policy with appropriate computer network management standards and protocols

It's tempting to blend a computer user policy with a computer network standard that's meaningful to the technology staff, particularly in areas of overlap like password management or security patches. Try to keep the computer use policy focused in areas of importance to all employees and make sure you have supplemental technology or network standards and protocols for technology staff to perform their work.

Be up front when it comes to monitoring employee use

Make sure the policy provides employees with notice that their files and communications are not private, that the city may monitor employee use and communications. Think about whether monitoring use will provide employees with a disincentive to tell you when they experience problems (for fear they might be disciplined). Consider how you will handle an investigation of employee behavior and what you will do with sensitive information you might uncover.

Think about additional policies or recommendations for elected officials

You may have elected officials conducting electronic conversations via e-mail or social media, creating documents or recording their information using technology tools. Be sure you think about how these documents and discussions are managed and merged with other city information. If the city provides equipment for elected officials, you might need to also communicate expectations and limitations about how that equipment is used.

Make the policy specific to your circumstances

A sample or model policy only helps to a certain point. Your city is probably operating a specific kind of anti-virus software, you may or may not have automatic updates of your operating system, your e-mail system may be different than another city's and your city probably has different uses for social media sites. The policy guidelines provided here are a place to start, but there's probably a fair amount of city-specific work that needs to be done.

Review the policy every year or so

Because technology and technology risks change so rapidly, you'll have to take a careful look at your computer use policy more frequently than other policies you may have.

Things to include

- When and how often staff can use city computers for personal reasons.
- Personal use that is acceptable and unacceptable.
- Who, other than staff, can use city computers (i.e., family members).
- Under what circumstances staff can access the Internet for personal purposes.
- Sorts of web sites staff can and cannot visit.
- Whether and to what extent staff can receive personal e-mail at city e-mail address.
- Precautions to take related to ongoing e-mail attachments.
- Appropriate e-mail and social media content, language, etc., for messages sent and received by staff, both personal and work-related.
- How to handle "spam" or junk e-mail.
- Appropriate passwords, how often they should be changed, where they should be stored, and with whom they can be shared.
- When to perform "maintenance" or "security patches" on computers (define those things in understandable ways).
- Types of software that can be downloaded or brought in and installed on city computers.
- Where and how to save city work, the city's records retention guidelines, and instructions for saving e-mail messages.
- Who may delete information or materials from the city computer network.
- Steps to take before using disks, recordable CD/DVDs, flash drives or other forms of removable media.
- Standards for encrypting confidential data on laptops and other removable devices, e.g., thumb drives, CDs, or DVDs.
- Appropriate use of remote access to city network resources if available.
- When and how staff may access the city network or data from home computer systems.
- Extent to which staff can customize look and operation of computer.
- When staff should tell someone at the city about a possible virus or other computer concern.
- How personal and business use of city computers will be monitored.

- Level of privacy staff has in conducting city or personal business on city computer system (the answer should be "none").
- Ramifications of violating the policy.
- How to protect the physical security of city computer equipment.

Sample policy

The following sample computer use policy is intended to be a guide for cities to develop city-specific guidelines for employee use of city-owned technology equipment and resources. Before using the provisions in this sample policy, a city may need to make changes or adaptations appropriate for its management style, staff resources and computer network structure. The sample reflects one set of solutions to the issues that a computer use policy should address, but different solutions might be a better fit in your city.

If you need additional suggestions for computer use policy language or would like to further discuss your city's policy provisions, please call the League's research department.

Specific things in the sample policy to check before using in your city include:

- Whether duties and functions identified as being performed by the city clerk, technology department and supervisor are appropriate for your city. For cities with a Human Resources director, some functions may be better performed by that role. Consider whether you want supervisors to play an additional role in enforcement of the policy.
- Whether the technical and vendor references to policy items like anti-virus software or allowable downloads are valid in your city (this policy references some vendors you might not use).
- What level of employee discipline is appropriate in your city for policy violations.
- Whether the file size for storing personal documents on a computer hard drive is appropriate for your city, whether you will allow personal documents to be stored on the city's equipment.
- Whether the city will allow storage of any personal files that contain copyright material such as mp3 files.
- What allowable software or system downloads you will permit, including security updates and patches to individual workstations.
- What other related policies should be referenced or attached (such as policies about records retention or data practices).
- How often you will perform back-ups of city e-mail and how long you will retain those back-ups. It's recommended that you back-up e-mail systems separately from all other system back-ups.
- Whether you will provide or permit any communication by Instant Messaging (IM).
- Whether you will permit access to social media sites for personal or city use.
- How you will store and manage protected or private information in accordance with data practices laws. It's recommended that you implement storage techniques to identify public and private data. Examples of such techniques include file structure standards, document naming conventions, or separate back-up systems for public and private data.
- What desktop tool you will use for anti-virus protection, including how employees will scan storage media such as floppy disks, USB drives, etc. Make sure the directions in the sample

policy fit your city’s practices for updates and resources (and that you change the name of software you use as appropriate).

- If you want to utilize encryption for files on removable media or laptops containing confidential information
- Whether you want to block any particular Internet sites or web protocols (traffic) from employee access.
- What password management guidelines you will use (required characters, password length, required change of passwords).
- How you will provide and manage remote access, including dial-up, VPN and webmail using city-provided, employee-owned or other equipment (such as a computer in a hotel lobby); and what additional instructions will be needed by employees for remote access.
- Whether there are other technology resource management standards or computer network protocols that need to be communicated to employees.
- Decide whether any additional policies are needed to address specific hardware or equipment issues in your city, such as a specific reference to use of city-provided PDAs or cell phones.

Your League Resource

Questions about computer use policies can be directed to the Research Department at the League by calling (651) 281-1200 or (800) 925-1122.

Greg Van Wormer 07/09

City of _____________

COMPUTER USE POLICY

Purpose

This policy serves to protect the security and integrity of the city's electronic communication and information systems by educating employees about appropriate and safe use of available technology resources.

The city reserves the right to inspect any data, e-mails, social media content, files, settings or any other aspect or access made by a city-owned computer or related system and will do so on an as-needed basis as determined by the city clerk.

All employees are responsible for reading and following information that may be distributed from time-to-time by the technology department about appropriate precautions to protect city systems.

An employee who violates any aspect of this policy may be subject to disciplinary action including revocation of certain system privileges or termination.

Personal use

The city recognizes that some personal use of city-owned computers and related equipment has and will occur. Some controls are necessary, however, to protect the city's equipment and computer network and to prevent abuse of this privilege.

- Only city employees may use city-owned equipment. Family members or friends of employees are not allowed to use city equipment or technology resources.
- Personal use must take place during non-work hours (breaks, lunch hour, before or after work). Personal use should never preempt work use.
- Reasonable use of city e-mail systems for personal correspondence is allowable, provided it does not interfere with an employee's normal work and is consistent with all provisions in this policy. Employees should treat this privilege as they would the ability to make personal phone calls during work hours.
- Reasonable use of the city's access to the Internet for personal reasons is allowable, provided it doesn't interfere with normal work and is consistent with all provisions in this policy.
- If an employee wants to use or connect their own peripheral tools or equipment to city-owned systems (such as digital cameras, PDAs, disks, cell phones, mp3 players or flash drives), they must have prior approval from the technology department and must follow provided directions for protecting the city's computer network.
- Files from appropriate personal use of the city's equipment may be stored on your computer's local hard drive, providing the size of all personal files does not exceed 50 MB. At no time may personal files that contain copyright material, such as mp3 files or photos, be stored on city computer systems. The city may inspect any data or information stored on its equipment or network, even if the information is personal to the employee.

- Use of city equipment or technology for personal business interests, for-profit ventures, political activities or other uses deemed by the city clerk to be inconsistent with city activities is not allowed. If there is any question about whether a use is appropriate it should be forwarded to the city clerk for a determination.

Software, hardware, games and screen savers

In general, all software and hardware required for an employee to perform his or her job functions will be provided by the city. Requests for new or different equipment or software should be made to your supervisor or directly to the technology department.

The following is approved software that may be downloaded by employees without prior approval:

- Microsoft updates as provided in automatic updates to the user.
- Anti-virus updates as provided in automatic updates to the user.
- Microsoft clipart and photo files.

Unapproved software or downloads (free or purchased), hardware, games, screen savers, toolbars, clipart, music and movie clips, other equipment, software or downloads that have not been specifically approved by the technology department may compromise the integrity of the city's computer system and are prohibited.

The technology department, without notice, may remove all unauthorized programs or software, equipment, downloads, or other resources if they could harm systems or technology performance.

If there is any question about whether software or hardware, downloads, etc. are appropriate it should be forwarded to the technology department for a determination.

Electronic mail

The city provides employees with an e-mail address for work-related use. Some personal use of the city e-mail system by employees is allowed, provided it does not interfere with an employee's normal work and is consistent with all city policies.

The city allows employees to access personal email accounts via the Internet provided such access occurs during non-work hours and fully complies with this computer use policy.

An employee's personal e-mail (and other personal documents) accessed via a city computer could be considered "public" data and may not be protected by privacy laws. Personal e-mail and computer use may be monitored as directed by the city clerk and without notice to the employee. Employees should not expect privacy in any activity conducted on a city-owned computer.

The following policies relate to both business and personal e-mail content sent from a city computer:

- Use common sense and focus primarily on using e-mail for city business. Never transmit an e-mail that you would not want your boss or other employees to read, or that you'd be embarrassed to see in the newspaper.

- Do not correspond by e-mail on confidential communications (e.g. letters of reprimand, correspondence with attorneys, medical information).
- Do not open e-mail attachments or links from an unknown sender. Delete junk or "spam" e-mail without opening it if possible, do not respond to unknown senders.
- Do not gossip or include personal information about yourself or others in an e-mail.
- Do not use harassing language, including sexually harassing language or any remarks including insensitive language or derogatory, offensive or insulting comments or jokes in an e-mail.
- All emails must comply with all city policies, including those related to respectful workplace, harassment prevention and workplace violence.
- Do not curse or use swear words in an e-mail.

Instant Messaging

The city does not provide employees with resources or tools to communicate by Instant Messaging (IM) when conducting city business. Employees are not allowed to use IM as a mechanism for personal communication through the city's computer network or when using city equipment, and are not allowed to download or install any IM software on their city computer.

Social Media

Cities should distinguish between use of social media sites such as Facebook and MySpace, blogs and microblogs such as Twitter, for official city business versus personal use. When using social media to support official city business in accordance with job duties, individuals should clearly identify themselves as connected to the city. Personal use of social media by city staff – whether about the city or not, and whether positive or negative – will reflect on the city as a whole. Personal use of social media should not violate any city policies already in existence, such as those on harassment prevention.

Storing and transferring documents

Electronic documents, including e-mails, electronic communication and business-related materials created on an employee's home or personal computer, should be stored on the city's network in accordance with city records retention policies and the Minnesota Data Practices Act. The following are some general guidelines that may be useful to consider:

- Electronic communication that is simple correspondence and not an official record or transaction of city business should be deleted as soon as possible and should not be retained by employees for more than three months. The city will not retain electronic communication longer than one year on the network or in network back-ups.
- Electronic communication that constitutes an official record of city business must be kept in accordance with all records retention requirements and should be copied to appropriate network files for storage.
- City-related documents that an employee creates on his or her home computer or any other computer system should be copied to the city's network files.
- Documents or electronic communications that may be classified as protected or private information under data practices requirements should be stored separately from other materials.

If you are unsure whether an electronic communication or other document is a government record for purposes of records retention laws, or is considered protected or private under data practices, check with your supervisor, the city clerk, or the designated responsible authority for data practices. If you are unsure how to create an appropriate file structure for saving and storing electronic information, contact the technology department.

Transferring data and documents between computer systems requires information to be stored on a floppy disk, CD-ROM, flash or USB drive, or other storage media. These items can also be used to transmit computer viruses or other items harmful to the city's computer network.

The city has installed anti-virus software on each computer to protect against these threats by automatically scanning storage media for viruses and similar concerns.

The anti-virus software provides automatic updates that employees will be notified of with a pop-up window from Symantec. All employees should follow directions for updating anti-virus software as prompted. If you have any questions about how to update your anti-virus software or check your storage media before you use it, check with the technology department.

Internet

The city provides Internet access to employees for work on city business. Employees may use this access for work-related matters in a professional manner.

Occasional personal use of the Internet is acceptable within the bounds of all city policies. The following considerations apply to all uses of the Internet whether business related or personal:

- There is no quality control on the Internet. All information found on the Internet should be considered suspect until confirmed by another source.
- Internet use during work hours must be limited to subjects directly related to job duties.
- Personal use of the Internet during non-work hours (breaks, lunch hour, before or after work) is permitted. However, employees may not at any time access inappropriate sites. Some examples of inappropriate sites include but are not limited to adult entertainment, sexually explicit material, or material advocating intolerance of other people, races or religions, or in manners that otherwise violate city policies related to respectful workplace and harassment prevention. This prohibition includes information on social media sites such as Facebook and MySpace, blogs and microblogs such as Twitter. If you are unsure whether a site may include inappropriate information, you should not visit it.
- No software or files may be downloaded from the Internet unless approved in advance by the technology department. This includes but is not limited to free software or downloads, maps, weather information, toolbars, music or photo files, clipart, screensavers and games.
- Employees may not participate in any Internet chatroom – an online meeting place to discuss a particular topic, sometimes in semi-privacy – unless the topic area is related to city business.
- The city may monitor any employee's use of the Internet for any purpose without prior notice, as deemed appropriate by the city clerk.

Passwords and physical security of equipment

Employees are responsible for maintaining computer passwords and following these guidelines:

- Passwords must be at least eight (8) characters long and include both lower and upper case characters, at least one number and at least one non-alpha-numeric character (e.g., *, &, %, etc.). An example might be Pol!ci3S.
- Your passwords should not be shared or told to anyone. If it is necessary to access an employee's computer when he or she is absent, contact the technology department.
- Passwords should not be stored in any location on or near the computer. If necessary, store your password in a document or hard copy file that is locked when you are absent from your desk. Do not store it electronically in a palm pilot or cell phone system.
- The computer system will prompt employees to update passwords every three months. Employees must change passwords when prompted.

Lock your workstation (press Ctrl-Alt-Del keys) if you will be away from your desk or office for more than five minutes. Unlock your computer by doing the same and typing in your password.

Use caution if you leave equipment unattended because it is generally small and portable. Do not leave city computer equipment in an unlocked vehicle or unattended at any off-site facility (airport, restaurant, etc.). If your office or desk area is in a high-traffic public area, check with the technology department about appropriate security measures.

Remote access

Certain employees may be given the ability to access the city's computer systems from remote locations or from home, using either personal equipment or city-owned equipment.

Remote access is limited to staff classified as exempt and who frequently work independently on city business. Non-exempt staff may be given temporary access from time to time as needed, but only with the approval of their supervisor, the city clerk and the technology department.

Employees with remote access privileges will be given specific instructions from the technology department about how to protect city equipment and information resources. If you have any questions about remote access to the city's network, check with the technology department.

Notice of computer problems

Employees are responsible for notifying the technology department about computer problems or odd computer behavior. Employees should err on the side of caution when reporting issues because small problems may indicate a more serious network or computer system issue.

Employee signature

I have received and read the above policies and have had an opportunity to ask any questions. I understand that my failure to follow these policies may result in disciplinary action including revocation of system privileges or termination.

____ ____

Print Employee Name

Print Department Name

____

Employee Signature

____

Date