



INFORMATION MEMO

Computer and Network Loss Control

Learn some of the risks in storing and sharing city data on computers, including portable devices. Find out how to protect the city from common risks such as data breaches, virus contamination, hacker attacks, and computer misuse by employees. Understand issues presented by social media such as Facebook, blogs, and Twitter. Links to a model employee computer use policy.

RELEVANT LINKS:

[LMCIT listserv for City IT Professionals](#) is a way to keep current on computer issues.

I. Elements of computer loss control

As more cities find ways to increase efficiency and communications through technology, the need for better computer security grows. Not doing anything could open the city to disastrous consequences. Even if a city has just one computer, if the city stores valuable data on the system, it probably will be exposed to computer threats.

Computer threats include private data exposure, and damage or destruction of software, hardware, or data from hacker attacks, employees, or viruses. There are also physical risks to your computers, network, and data from disasters like fires, physical damage, or floods.

Recommendations discussed in this memo are not a guarantee that your computers and network will be completely safe from harm, but actively managing these risks and keeping up with new developments in this area will go a long way toward controlling computer-based losses.

II. Security risks

A. Physical and electronic security

You can have the best policy in place and trustworthy city staff, but that does not protect you from computer security risks. Even though most city data is public, it needs to be protected from accidental or malicious deletion. This is similar to paper files in that they may be public data, but you wouldn't put the file cabinet in front of city hall for anyone to browse or remove files. Simply locking the file cabinet wouldn't prevent someone from stealing the entire file cabinet or destroying it.

Security threats may come from inside or outside your city. Internal threats include but are not limited to disgruntled employees, untrained employees, or former employees whose access has not been removed. External threats include but are not limited to hackers, viruses, phishing scams, and malware.

This material is provided as general information and is not a substitute for legal advice. Consult your attorney for advice concerning specific situations.

B. Virus or malware contamination

Virus contamination of computer systems is a large risk. Many viruses are undetectable without anti-virus software, and could be present for years without showing any signs of malice. Viruses or malware can cause issues in many ways. The most obvious is they could destroy city data that could be costly to restore or recreate. Other viruses may capture keystrokes or passwords and utilize them maliciously. Viruses could also allow hackers to gain unfettered access to a city's network, where data could be read, deleted or, in some cases, encrypted and held hostage for a fee. Finally, they could attack a city's network causing connectivity to become slow or unusable. Viruses replicate and can move from computer to computer via networks, email, flash drives, CDs or DVDs, or even smart phones that were created or accessed by an infected computer. If a city does not take measures to ensure a virus-free network, and private data is exposed, the city could end up in litigation for the data breach.

C. Hacker attacks

Poor security may allow a hacker attack of the city's computer system. A hacker may obtain private data, opening the city to a lawsuit by the subject of the data for allowing the data to become public. City data may also be destroyed or modified. A hacker can hijack the city's system to use it for a "denial of service" attack on a third party. The affected party may in turn sue the city for carelessness in allowing computers to be so easily commandeered by the hacker. Hackers may also turn computers into mail servers that send out spam email, which could cause a city's email domain to be blacklisted. This means very few email messages from city email accounts would make it to the intended recipient.

D. Physical losses

A city may lose data and software from an accident, natural disaster, or other event. Examples include fire, tornado, flood, lightning strike, building collapse, riot, vandalism, or theft. Any of these could leave a computer or network in a state where data cannot be recovered.

E. Cloud computing

Cloud computing is the "delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet). Clouds can be classified as public, private, or hybrid."

Wikipedia, [Cloud Computing](#).

RELEVANT LINKS:

Cloud-based applications provide some potential risks, not because they are cloud-based, but because they may not be configured appropriately, or data may be stored in a way that conflicts with data practices. If a cloud provider doesn't handle data correctly, the city still could be liable for loss or release of data even though it was handled by the cloud provider.

F. Computer or social media misuse

Misuse of computers, such as a city employee using the city's computer to send harassing emails, can create liability for the city. Likewise, an employee may sue the city for looking at emails the employee sent or received on the city's system, claiming that she expected those communications to be treated as private.

Social media is another area where misuse can become an issue. Because of the prevalence of social media outlets such as Facebook and Twitter—accessible through an Internet connection—city employees may have their own social media accounts, where they may write things about work.

City officials should care about social media even if their city doesn't yet have an official Facebook page or Twitter account. The lines between personal and work lives are getting blurrier each day. For better or worse, at some point an employee's personal social media activity will relate to something that happened at work. You need to help employees identify what is appropriate and inappropriate content related to city business. Good guidelines are important to keep employees—and the city—out of trouble.

G. Websites and social media information

Material the city posts on its website may open the city to risks such as release of private data or wider harm such as damage to city facilities. For example, the city pinpoints the location, size, and design of the city's water system facilities or emergency response practices. This information is then used by terrorist or anti-city organizations to plan an attack

Social media primarily are Internet and mobile-based tools for sharing and discussing information. While accessible through the Internet, social media is generally thought of differently than a city website. A city website is the official voice of the city and is recognized as such. Cities typically assign website content development and posting duties to staff as part of their official job duties. Sometimes those duties include a supervisor's review of content before it is posted to the website. Where content sign-off isn't required, communications or other guidelines usually direct staff in the city's standards and expectations for acceptable and unacceptable website communications.

H. Demands for data

In a lawsuit or other data practices requests, a discovery demand for information will most likely include all the city's relevant email and other electronic data. Backup media may be part of the request. The city may be compelled to spend significant time and money looking for the relevant data on all systems, and redacting any non-public information. Data requests may also cover a personal computer or other technology, including personal devices used to conduct city business, or social media data that have been used to communicate on the topic of interest.

I. Disability claims

Poor ergonomics when using computers may result in employee worker compensation claims for a repetitive stress syndrome injury. These claims can be expensive and may result in permanent disabilities.

J. Staffing

People who maintain the city's network may not understand data practices issues, or may not have an appropriate skill set to ensure electronic records are cared for appropriately. Poorly trained information technology staff could also unknowingly expose a city's network/computers to virus attacks or security breaches. Poorly vetted staff could steal/damage equipment, data, or software.

K. Portable devices

As portable devices become more prevalent in the workplace, it is important to consider them when thinking about loss control. What defines a portable device? The definition of portable devices includes any medium that can access city networks, systems, or emails. Some examples are smartphones, iPads, tablets, and netbooks.

Address portable devices under the city's Computer Use Policy. The policy must cover all employees and elected officials conducting city business on portable devices. As part of the policy, password protection on the devices should be required. For example: Why should employees and elected officials make it a habit to clean the screen on their portable devices?

Answer: Over time, oils from fingertips can accumulate on the device screen and create a discernable pattern potentially marking the password for that device. Portable device training must include:

- Why passwords are important.
- Data practices considerations with portable devices.
- Ways to secure the devices.
- What steps to follow if a portable device is lost or stolen.

RELEVANT LINKS:

Office of the State Auditor
E-Update, Feb. 13, 2015.

The Office of the State Auditor has these recommendations about portable devices:

“Notebook computers, USB flash drives, and other removable media devices are often used outside a secure network environment, which makes them particularly susceptible to loss. As a result, extra care needs to be taken to protect the devices and any ‘not public’ data contained on them.

“All computers should be secured with a strong password. To protect both the data and the computer equipment, the following security measures should also be considered:

- Government data should not be stored on personal computers, personal USB flash drives, and other similar personal equipment.
- ‘Not public’ data should be stored on a notebook computer or removable media device only when there is a business need.
- Data stored on a notebook computer or a removable media device should be strongly encrypted.
- When removable media are no longer in use, they should be securely destroyed.
- When disposing of computers, the hard drives should be securely erased.
- Cable locks should be used for all computers, except while in transit.
- Computers should never be left in an unattended vehicle.”

L. Removal from service

Consider portable devices when creating the policy guiding the procedures for taking technology out of service. Quite a number of devices/machines store information on the hard drive. It is essential that the hard drives are either removed, wiped, or destroyed when the equipment gets removed from service as the hard drive may contain private data. Public entities need a written policy that addresses the disposal of these items and the specific process for destroying the information on the hard drives. Devices to consider including in this policy:

- Copiers/scanners
- Fax machines
- Computers
- Portable devices (phones, tablets, laptops, netbooks, etc.)

III. Reducing computer security risks

A. General security

Security of a city’s network needs to be addressed in three areas: physical, data, and personnel.

RELEVANT LINKS:

See, Wikipedia, [Social Engineering \(Security\)](#) for some current examples of this type of social engineering.

Servers, switches, computers, laptops, and other data devices should all be secured from physical threats such as theft or environmental damage.

Data should be secured by granting rights only to people who require access to the data. This is usually done through a system of folders and sub-folders, with appropriate security applied. This is called data mapping and is covered later in this document.

Employees should have their own computer accounts granting them access to only the data they require to complete their duties. When staff leave employment, their accounts should either be deleted or, if it's an account that will be moved to a new staff person, the password should be changed. Passwords should be required for all accounts and should be complex passwords or passphrases.

Shared and administrative passwords should be changed annually, or when an employee who has access to the password leaves employment with the city.

City staff and elected officials are also key to computer security. Social engineering, that is, the psychological manipulation of people into performing actions or divulging confidential information, is quickly becoming one of the easiest ways for hackers to gain access to networks. City staff should be made aware of the methods used and be trained in simple security measures such as not sharing passwords, not writing them down and keeping them close to the computer, not emailing them, and not giving them out to anyone other than verified support personnel.

B. Anti-virus software

Ensure all devices used for city business (including ones at home if used to do city work) have current, updated anti-virus software installed. There are many vendors that offer anti-virus products and the choice of which software is the best to use will vary from city to city. A reputable company that provides support in the event of a virus outbreak should be chosen. Some vendors offer "free" anti-virus software such as AVG or Microsoft. These free programs are usually only free for personal use so, in theory, cities would have to pay for the product if they choose to use it.

C. Firewalls

Any connection to the Internet should be protected by a firewall. Hardware firewalls are usually provided by your Internet service provider. However, these are often simple firewalls that offer only basic protection. Cities should consider purchasing their own firewall and having a technology professional configure it to meet their needs.

RELEVANT LINKS:

For additional information about encryption see Wikipedia, [Encryption](#).

The default configuration of a firewall should never be used. A default configured or misconfigured firewall is almost as bad as not having one.

In addition to a firewall at the point of connection to the Internet, computers should also have a software firewall configured. This is especially important for tablet and laptop computers, since they will most likely be using Internet connections not controlled by the city (e.g., hotels, coffee shops, and home connections).

D. Data encryption

While the majority of city data is usually considered public, encryption is critical for private data. Any mobile device or laptop that contains private information should have its storage media encrypted. Examples would include a smartphone with private emails, or a laptop containing private data. Servers generally do not require encrypted media, since they should be stored in a secure physical location. However, it is slowly becoming a best practice to encrypt server data as well. While less critical than securing end-user devices, it's another layer of protection for city data.

External connections, such as VPN or webmail, should also be encrypted.

E. Wireless security

No wireless access point should ever be considered secure. Even "secured" access points that require passwords and that are encrypted can be easily compromised by hackers. City staff should be trained on not transmitting private data over wireless networks.

F. Cloud computing

Before storing any city data in a cloud-based application, it is paramount to review the usage agreement for the service to ensure data is stored appropriately. You also want to make sure that, if you are required to produce data under a data practices or e-discovery request, it will not cost too much for the city to pull the information back. This is especially important for how the data is backed up. In some e-discovery cases, backups of data were considered accessible data and needed to be produced.

G. Staffing

Appropriate and trained staff should be responsible for maintaining a city's network and computers. Most cities cannot afford a full-time technology professional and will need to rely on consultants. Regardless of whether that person is a contractor or city employee, a city must make sure the person has passed an appropriate background check.

RELEVANT LINKS:

[Minn. Stat. § 13.05, subd. 5.](#)

State of Minnesota,
Information Policy Analysis
Division, sample [Policy for
Ensuring the Security of Not
Public Data](#).

[Minn. Stat. § 13.055, subd.
1-6.](#)

[Minn. Stat. § 13.09.](#)

(Most technology vendors require background checks and will provide documentation that they performed the check upon request). Using a high school student or relative of a city official is probably not a good idea unless they are a true technology professional.

Any staff responsible for maintaining a city network should also be aware of data practices issues, and should understand the concept of the city's records retention schedule.

Technology staff should generally not be the people tasked with records retention duties, but should be familiar enough with the process to advise a city on storage methodologies.

H. Data mapping

Data mapping is critical to keeping a network organized and reducing costs in the event of e-discovery. All city staff should be aware of the data mapping architecture. (In smaller cities, this may be as simple as a few folders on a computer such as, "Public Data," "Private Data," and "City Council Information"). Security should be applied to these folders as well. For example, personnel data should be stored in a separate folder where only city staff tasked with HR responsibilities can access it. Other data that is more public in nature would then be stored in a separate folder or area with less restrictive access. How this is set up may vary from city to city. However, having an overall plan for where data is stored is critical. Failure to protect private data appropriately is a violation of state statute.

Cities must establish security measures to help ensure that private data "are only accessible to persons whose work assignment reasonably requires access to the data, and is only being accessed by those persons for purposes described in the procedure." In addition they must follow data breach laws, and they must perform an annual security assessment of "personal information" the city maintains. Accessing private data without authorization is a misdemeanor, and a willful violation by a public employee is just cause for suspension without pay or dismissal.

I. Patches, service packs, and upgrades

Patches, services packs, and upgrades need to be applied regularly to all operating systems, anti-virus clients, networking equipment, software applications, and any embedded equipment that connects to the Internet such as water/wastewater systems or security systems. If possible, updates to end-user equipment should be automated, and end users should not be given a choice of running the updates.

RELEVANT LINKS:

Updating embedded systems will often require more vendor interaction and cost, so the risks of not updating the systems should be weighed against the cost of potential breach. For example, the malicious turning off of the pump in a lift station may be a greater risk than the malicious shutdown of the system that handles the lawn sprinklers for the library.

J. Data backup

Regularly back up the data on the city's computers, and conduct tests to ensure backups are not corrupted. The city should back up all data to protect itself from natural disaster, failed hardware, viruses, or hacker attacks. Backup media should be stored in a secure, climate-controlled, off-site location. The location should be far enough away such that a natural disaster such as a flood or tornado would not be likely to take out both the equipment being backed up, and the off-site storage location. Storing backup media in the back of a public works shed would probably not fit the definition of a secure, climate-controlled, off-site location.

The city should establish a regular backup schedule addressing frequency of backups and retention of backup media. Backups should be done on a daily basis. A complete monthly backup should be maintained on a 12-month rotating schedule. Ultimately, the type of schedule really depends on the size of the city and the kind of operations housed in the system.

Specifically address how emails and backup tapes containing emails are handled in the city's records retention schedule. Cities should back up email separately, so that emails aren't retained indefinitely along with other city data that has a longer retention need. A separate email backup also ensures any archived electronic city records do not need to be searched as part of an email eDiscovery ordered by the court.

Backup media should be replaced on an annual basis. Most backup media will deteriorate after a year of use.

K. Computer use and social media policies

Adopt a computer use policy, and ensure all staff are aware of the policy. Make sure it includes use of social media for personal and professional purposes. Decide whether the city has an official presence in social media, and whether you will use a centralized or decentralized strategy. Make sure city employees are aware of the policy, and consistently enforce it. Consider voluntary policy language to govern elected officials' use of social media and other electronic communications.

See Section IV, *Developing a computer use policy social media policy*, and Section III-L, *Website and social media policies*.

LMC information memo, *Meetings of City Councils*, Section II-G-8, "Telephone, email and social media".

RELEVANT LINKS:

LMC Model, [Computer Use Policy](#).

LMC Model, [Social Media Policy](#).

L. Website and social media policies

Think about the kind of information posted on the city’s website.

Recommendations include making sure there is no private data, and that data is accurate. Even if data is legally public (e.g., the location, size, and design of your water system), it may not be a good idea to post it on the website.

Only post information that is legitimately useful to citizens and constituents.

Social media largely is perceived as a less formal method of communication than a website. Cities that are using social media to communicate official city-sponsored messages should be managing that official social media content in much the same way they manage the city newsletter or website.

The following are recommendations to help cities avoid problems related to social media.

1. Social media as a city business tool

Because social media is relatively new, experts are only now beginning to understand the associated liability issues. Cities should be mindful that any forays into social media—whether as an official voice of the city, voice for elected officials, or as personally used by staff—could create an embarrassing situation for the city. Above all, employees should consider anything they post to be permanent and public. It is a good idea to advise employees to refrain from sending or posting information that they would not want their boss or other employees to read, or that they would be embarrassed to see in the newspaper.

In some instances, the city could face legal challenges if incorrect, false, or non-public information is posted on a site used officially by the city or personally by employees or elected officials. In other settings, the city may face data requests that could include content posted to social media sites on city and/or personal computers, depending upon where content was posted and who posted it.

Before considering social media use as a tool for city business, a city should weigh benefits against risks. Answering the following questions will help set a course for identifying who should speak for the city, when the city wishes to use social media, where it wants to engage, and more.

a. Is social media different from the city website?

Social media is different from a city website. The city’s website functions as an official voice of the city. Often city websites include formal communication about city events, projects, policies, and ordinances.

City websites primarily are one-way forms of communication where cities “push” information out to the public, and websites rarely offer opportunities

RELEVANT LINKS:

[“Two-Way Street: What is your City’s Approach to Social Media,” *Minnesota Cities* \(May-June 2013\).](#)

to directly comment on information on the site. Most sites offer email addresses for visitors to send comments to.

Social media can be used as an official voice of the city, but it’s different. Social media can be accessed simply, through the Internet.

One of the primary goals of social media is to encourage two-way communication. Information shared in a social media setting typically happens in real time. Social media information is “pulled” by followers. Simply put, in social media, people choose who they want to connect with by deliberately “following” or “friending” them. The act of following someone on a microblog or friending someone on Facebook means that when they visit their accounts, they will see information posted by the people, groups, and organizations they follow, and can comment right away on what they see, hear, and read—they can have a conversation in real time.

b. Should the city use social media?

Determining whether social media is a good way for the city to communicate with residents is an individual city decision. Factors that may impact a city’s decision could include staffing levels, communications needs, overall city goals, technology support, staff interest (or lack of interest) in social media, and other unique considerations.

In some instances, social media may complement current communications vehicles such as newsletters and the city website, reach audiences the city otherwise wouldn’t connect with, or replace (partially or fully) some existing communications tools. It might even help the city gather valuable input from residents about programs and services, or communicate emergency messages.

When considering how to integrate social media, the city should consider whether electronic media can actually replace print media. It’s likely that not all residents have access to electronic forms of communication, so eliminating some of the city’s existing communications tools could actually decrease its ability to connect with residents. It’s also important to think about what types of communication to distribute via social media as each is developing a niche. Currently, microblogs are emerging as a tool for making announcements about such things as upcoming meetings and events, communicating with people in real time and on the go, and learning what others are doing or saying; blogs are being used to relay information that is more subjective in nature; and sites such as Facebook are being used for sharing information and photos.

c. When should the city use social media?

There are many opportunities for a city to use social media in an official manner. Ultimately, the answer depends upon each city.

RELEVANT LINKS:

Some cities might choose to use social media to announce upcoming changes to services such as swimming pool hours or additional ball fields; provide updates on projects such as street improvements and skate park construction; announce city-related festivals; provide in-depth information on certain policies such as assessments and zoning; gather feedback and input from residents on projects, services, and ordinances; or any number of other city-related topics.

d. What social media tools should the city use?

The tools a city chooses to use will depend upon the type of information the city wants to communicate. Generally speaking, different tools work well for different types of things.

(1) Microblogs

Microblogs such as Twitter work well for taking the pulse of current events such as breaking news and legislative policy issues. Microblogs also work well for sharing announcements about projects such as a street being closed for resurfacing, reminding residents about parking rules during snow emergencies, and registration opening for parks and recreation programs. The value of microblog comments is enhanced when links are included to more information about the projects, policies, and programs that are already posted on the city website. Microblogs can also work well for getting a snapshot of what people are thinking about at the moment to help get a sense for a trend. Carefully cultivating who a city follows can help increase the visibility of the city among groups such as the media, political leaders, and residents.

(2) Social networks

Social networks, such as Facebook, work well as a gathering place for people interested in the city, and for building affinity for the city. Social networks can serve as a place to post information and pictures of a community celebration, a project that succeeded because of volunteer efforts, or even of various city staff performing interesting aspects of their jobs. These spaces also could be used to gather input and ideas from residents on projects, services, and ordinances.

RELEVANT LINKS:

(3) Video sites

Video sites, such as YouTube, Vimeo, and iReport, allow users to post, rate, and comment on videos. Posting videos can be a way to provide a comprehensive picture of a city event, such as award ceremonies, and even be a virtual way to show residents the range of work done by city staff. (Videos shouldn't be posted of any individual without that person's knowledge and consent).

(4) Photo sharing sites

Photo sharing sites, such as Flickr and Instagram, allow users to post, rate, and comment on photos, can help create a comprehensive picture of a city event such as award ceremonies, and even be a virtual way to show residents the range of work done by city staff. (Photos shouldn't be posted of any individual without that person's knowledge and consent).

(5) Wikis

Wikis, such as Wikipedia, can be used to develop information on a range of topics such as about the city's founding residents, historic sites, and so on. Wikis are encyclopedia-like applications in which entries are created and edited by multiple people.

2. Centralized or decentralized approach to social media

A city should consider whether it wants an official social media presence and, if so, in what social media venues. The city should think about when and how it wants to use social media, whether to have an official city voice, and whether to use a centralized or decentralized approach. The manner in which social media fits with other official forms of communication also should be considered.

It may be the case that having multiple city social media users—or a decentralized approach—makes sense for a city because it allows subject matter experts to talk about issues related to their areas of expertise. For example, the city clerk might blog about changes to polling sites and announce openings for various committees and commissions, while the police chief talks about the city's K-9 officer. Microblogs might be used by public works staff to alert residents to snow parking emergencies, while parks and recreation staff announce enrollment openings for new programs.

A consolidated—or centralized—approach assigns social media responsibilities to one or two people. Depending upon the city, this approach could create a significant workload for those individuals, who may not have the time to support such a task. On the other hand, a centralized approach probably would provide the city with a more controlled, consistent, and uniform social media presence.

RELEVANT LINKS:

Handbook, [Chapter 27](#).

LMC model, [Computer Use Policy](#).

LMC model, [Social Media Policy](#).

3. Records retention

Keep the Minnesota Government Data Practices Act in mind when using social media. Much of what is posted likely does not need to be kept unless it serves as the official record of government action.

For example, a posting announcing an upcoming registration for a city program has a link to a downloadable form on the city website. If the city is linking from social media to an official government record posted on the city website, the records retention schedule likely applies to the record itself and not the website or the social media outlet in which the link was posted. The communications medium doesn't change the nature of a government record.

It's important that cities remember that if they keep something not required under records retention, such as a transitory email or Facebook message that is not an official government record, it would still be considered government data and probably classified as public. So, to the extent a city keeps more than it is required to keep, the city may have to produce that information.

Not all information posted will be conversational, of course. Some information will be official in nature and, therefore, will need to be maintained. An example might be taking public comment via the city's Facebook page or Twitter account on a proposed development in the city.

IV. Developing a computer use and social media policy

An effective computer use policy takes a comprehensive look at employee use of a city's technology. It governs employees' use of city-provided technology resources, including city-managed email; electronic communications; social media and Internet access; precautions to take against things like computer viruses; and consequences for breaking the policy.

Ideally, a computer use policy is 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.

A good computer use policy can:

- Ensure city staff understand technology responsibilities.
- Protect city technology and data assets.
- Increase employee productivity by not having to clean up things like virus outbreaks and junk emails.

RELEVANT LINKS:

- 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.

A. Human resources concerns

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.

1. 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.

2. 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.

3. Focus on education

Most employees won't deliberately introduce viruses or other nasty stuff into the city's computer system, but the majority of them might not understand how visiting a website for online gaming 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 employees about the policy you've put in place.

4. Simplicity

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. For example, should you include rules about city-owned cell phones in a computer use policy or create a stand-alone policy for phone use?

RELEVANT LINKS:

LMC information memo, [Meetings of City Councils](#), Section II-G-8, "Telephone, email and social media".

5. User policies versus network standards

Supplement the computer use policy with appropriate computer network management standards and protocols. It's tempting to blend a computer use 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 on 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.

6. Employee monitoring

Make sure the policy provides employees with notice that their files and communications are not private, and 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.

7. Elected officials

You may have elected officials conducting electronic conversations via email 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.

B. Technology concerns

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. The League recommends yearly review.

1. Items to include

An effective computer use policy should include the following:

- 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 (e.g., family members).
- Examples and types of websites staff can and cannot visit.
- Whether and to what extent staff can receive personal email at city email address.

RELEVANT LINKS:

- Guidelines for appropriate email and social media content, language, etc., for messages sent and received by staff, both personal and work-related, including following city respectful workplace, data practices, and political activity policies.
- How to handle “spam” or junk email.
- Appropriate passwords, how often they should be changed, where they should be stored, and with whom they can be shared.
- Guidelines on software procurement and installation.
- Where and how to save city electronic data, including email, and a mention of the city’s records retention schedule.
- Whether or not removable media, such as portable disks, DVDs or flash drives, is allowed. If allowed, steps to take before using disks, recordable CDs/DVDs, flash drives, or other forms of removable media.
- Standards for encrypting confidential data on laptops and other removable devices, e.g., portable drives or flash drives.
- Appropriate use of remote access to city network resources if available.
- Whether staff are allowed to access the city network or data from personal computer equipment.
- How personal and business use of city computers will be monitored.
- Level of privacy staff have 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.

2. Customizing your policy

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 email system may be different from another city’s, and your city probably has different uses for social media sites.

The League’s model policy guidelines are a good place to start. 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.

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

See LMC *Model Computer Use Policy*.

RELEVANT LINKS:

- 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 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 software or system downloads you will permit, including security updates and patches to individual computer equipment.
- What other related policies should be referenced, included, or attached (such as policies about records retention or data practices).
- How often you will perform back-ups of city email and how long you will retain those back-ups. It's recommended that you back up email 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.
- Whether 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 mobile devices, VPN, and webmail.
- Whether you will allow personal computer equipment to be used for conducting city business. If you do allow it, you should include a statement notifying employees that if personal equipment is used for city business, it may make the equipment discoverable for data practices purposes or e-discovery purposes.
- Whether there are other technology resource management standards or computer network protocols that need to be communicated to employees.

RELEVANT LINKS:

LMC Model, [Social Media Policy](#).

LMC Model, [Fire Department and EMS Social Media Policy](#).

C. Social media

1. Included or not

Determine whether you want to incorporate your social media policy into your computer use policy, or create a separate policy. The more official use of social media permitted, the more likely a separate policy is needed.

Some city functions, such as the fire department or EMS, may benefit from additional social media policies tailored to their unique work duties and situations.

2. Official city presence

An official city presence in social media probably would be dedicated to communicating information only on official city business such as upcoming city council meetings and events, programs in the parks and recreation department, public works projects like road closures, and so on.

The city would determine whether it wanted a centralized or decentralized social media strategy. A centralized strategy would have a single department or person responsible for all official social media postings. Decentralized would allow various departments or staff to communicate their individual postings.

Regardless of which strategy is chosen, there should be an official list of who is allowed to represent the city in social media. Among other expectations, staff with social media responsibilities would be expected to avoid posting information or comments that are critical, false, or disparaging, or could be damaging to the city's reputation.

Access to social media sites through city technology and during regular work hours would be approved, and may even be allowed from personal technology so that timely postings to social media can happen in accordance with the city's guidelines. For instance, an employee in charge of using social media for snow emergency plowing notices might need to access the city social media sites after normal hours and, therefore, would be allowed to do so from home or from a web-enabled phone. When staff are assigned to serve as the official voice and required to access social media after hours, the city should consider what posting official city business from personal technology means in the context of the city's records retention policies. It might make sense to encourage that any communications related to official city business be retained in a separate file so that it is easy to produce all city-related business information posted to social media should there be a request made under the Minnesota Government Data Practices Act for all communication related to a particular topic.

RELEVANT LINKS:

It also would be helpful to provide etiquette guidelines for expected behavior by staff charged with using social media on behalf of the city. Etiquette guidelines might include the following:

a. Account names

General social media pages, such as Facebook pages should clearly indicate they are tied to the city. Staff charged with representing the city could be expected to clearly illustrate on their account that they work for the city. This could be done by requiring all staff who use social media to include a city-designated prefix on their account names, much like the conventions set up for email years ago. For example, if John Doe, the public works director, is maintaining a public works Facebook page for the city, the page might be named “Mosquito Heights Public Works John Doe” and his Twitter account might be “MH-JohnDoe.” Sally Deer, the clerk, might be “Mosquito Heights Clerk Sally Deer” on Facebook and “MH-SallyDeer” on Twitter. Profile information for pages maintained by designated staff should include staff’s city job title, and could include the city’s website address, street address, and other relevant information.

b. Transparency

Personal opinions don’t belong in an official city social media communication unless the city has asked a person to share personal views and comments.

If that’s the case, the person sharing his or her comments should clearly identify the comments as the poster’s own opinions, not those of the city. A good precautionary principle for the city and it’s official communicators to follow—regardless of the city policy on posting opinions—is that if you’d be embarrassed to see your comment appear in the news, don’t post it.

c. Honesty

When posting information on social media, city representatives should be honest, straightforward, and respectful while being mindful of the need to maintain confidentiality and privacy when appropriate. Individuals should be sure that efforts to be honest don’t result in sharing non-public information related to co-workers, personnel data, medical information, claims or lawsuits, or other non-public or confidential information. Where questions exist, staff should consult with their supervisor or city attorney.

d. Mistakes

If a city representative makes a factual mistake on social media, the individual should correct it as soon as he or she is aware of the error. Corrections should be upfront and as timely as possible.

RELEVANT LINKS:

LMC Model, [Social Media Policy](#).
LMC Model, [Fire Department and EMS Social Media Policy](#).

If the individual is correcting a blog entry, the author may choose to modify an earlier post, and make it clear the posting has been corrected.

The web contains a permanent record of mistakes, so attempting to disguise a mistake likely will make things worse.

To prevent errors, a city employee should fact check official communications before they are posted in social media. Potential errors could create city issues ranging from minor to significant, and some may create unforeseen liability issues.

For example, posting to Facebook the wrong opening date for enrollment in a parks and recreation program likely will create confusion, inconvenience, and even frustration among residents who try to enroll their kids in a program too early and essentially end up wasting their time, or who find a program full because they tried to enroll their kids too late for a program. It's unlikely this type of mistake would create city liability.

But posting incorrect information about a new city ordinance related to land use zoning stands a greater chance of creating liability if someone acts based upon that incorrect information, and later is penalized for the action they took based upon the incorrect information officially posted by the city.

e. Legal requirements and city policies

Make sure not to post material that may violate federal or state laws. Follow city guidelines closely. Examples of cautions in this area include the following:

- Do not upload, post, transmit, or make available content you know to be false, misleading, or fraudulent. All statements should be true and not misleading. Do not post photos that infringe on trademark, copyright, or patent rights of others.
- Non-public and confidential information such as information related to co-workers, personnel data, medical information, claims, or lawsuits against the city should never be shared. Posting such information could create liability issues for the city and the person posting the information.
- Do not post content that violates existing city policies, that exhibits hate, bias, discrimination, pornography, libelous, and/or otherwise defamatory content.
- Only post content that is suitable for readers and viewers of all ages. Do not post content that a reasonable citizen may not consider to maintain the dignity and decorum appropriate for government. Do not post information that affiliates the city with or advocates for a political party or candidate running for council.

RELEVANT LINKS:

LMC model, [Social Media Policy](#).

LMC Model, [Fire Department and EMS Social Media Policy](#).

- Do not post any photo or video without permission of each person in the photo or video. Do not post the name of any individual without permission from that person.

f. Third-party sites

Only post to third-party sites when it is relevant to the city.

g. Media contact

Employees who are contacted by the media should follow city media relations/communications protocols.

3. City staff personal use

City staff without official social media responsibilities likely use social media to keep in touch with friends, family, colleagues, and groups with mutual interests. As part of their personal use of social media, it's not difficult to imagine that sometimes city staff may comment on city-related issues. Such a scenario often starts out innocently enough, but can lead to problems down the road.

An example of use of a personal social media account that crosses the line from strictly personal to city-related could be of the public works director who has a personal Twitter account. The public works director created the account to talk about and follow others with shared interests on topics such as hobbies, raising kids, and professional sports.

After being on Twitter a while, the public works director finds an official account for a professional group that he belongs to—the American Public Works Association. He already regularly visits the APWA website, but following the APWA on Twitter means he gets real-time updates about things that impact his job—national wastewater rule changes, upcoming conferences, and job openings. He's now started to merge his personal and professional lives.

Now consider that he's developed a following on Twitter that includes his friends who live in the city, and some of their friends start to follow him. One day the public works director realizes he has a broad network of people interested in what he has to say, and some folks are following him just because he works for the city.

He starts to see Twitter as a way to communicate important information to residents about snow emergencies or ice rinks opening, and he does so. His following grows because people know they can get important city-related news when it matters most.

RELEVANT LINKS:

At first, the city information being communicated is straightforward, doesn't bear any real negative impact for the city, and actually helps the city do its work—residents are moving their vehicles before plowing begins!

a. Employee right to speak publicly

This is not a new issue. Employees have always had the ability to communicate on city issues. Previously, employees could write a letter to the editor or circulate a flyer. However, social media has dramatically increased the speed, audience size, and impact of these communications.

In the scenario above, the city should still consider what it means that the public works director has started to use personal social media for official city business. The city could determine it would like to make use of social media part of the public works director's official job duties. Some questions to consider in this scenario include:

- What happens if the public works director is disgruntled because a new equipment request is denied, and he posts information blasting the council?
- What if he comments negatively about a staff member, or shares non-public information about that person in his personal social media accounts?
- What happens if the city faces a data request, and a personal computer or other technology has been used to communicate on the topic of interest?
- What happens if he takes a job in another city, and the city loses those connections to the public that he developed via social media?

City staff generally have the right to speak publicly as private citizens on "matters of public concern." Such speech, even if made in the workplace or as part of official duties, may be constitutionally protected if the interests of the employee, in commenting upon matters of public concern, outweigh the city's interests in promoting the efficiency of the public services it performs through its employees. Be careful to balance these interests before taking any action against an employee for the content of the speech he or she publicizes on social media sites. Of course, not everything is defined as a matter of public concern—comments on private matters with no impact on the greater public generally are not considered protected speech. Cities should consult with their city attorneys as appropriate on this issue. Staff never have the right to reveal non-public or private data.

b. Etiquette guidelines

Etiquette guidelines for staff who use social media on a personal basis might include the following:

RELEVANT LINKS:

(1) Account names

Personal social media account names should not be tied to the city. This will help clarify that the individual is not speaking officially on behalf of the city. For example, the personal Twitter account for John Doe, the Mosquito Heights public works director, should be just “JohnDoe,” his Facebook page “John Doe’s,” and so on.

Staff interested in using social media officially on behalf of the city should talk with their supervisor.

(2) Legal requirements and city policies

Individuals who use personal social media accounts are not immune from the law, or from the need to follow existing city policies and guidelines related to harassment prevention, media relations, computer use, and other city policies. Examples of cautions in this area include the following:

- Individuals should be encouraged to refrain from uploading, posting, transmitting, or making available content known to be false, misleading, or fraudulent. They should be encouraged not to post photos that infringe on trademark, copyright, or patent rights of others.
- Individuals never have the right to post non-public and confidential information such as information related to coworkers, personnel data, medical information, claims, or lawsuits against the city.
- Individuals should not use city-owned equipment to post to personal sites content that violates existing city policies, that exhibits hate, bias, discrimination, pornography, libelous, and/or otherwise defamatory content.
- Individuals should be encouraged to post to personal sites only that content which is suitable for readers and viewers of all ages.

4. Elected officials’ social media use

Some elected officials already use blogs, microblogs, Facebook, and other social media to connect with constituents and to promote political agendas. This is a reasonable use of social media, but elected officials should not use official city social media sites for campaigning purposes, just as they would not use the official city website or newsletter for campaigning.

It would be useful for elected officials to consider the effect personal comments about official city business can have on the city as a whole. Just as with face-to-face comments, electronic comments via social media can serve to “stir the pot” when an official speaks in opposition to an official city position adopted by a vote of the council. The city council might consider voluntary policy language to prevent this kind of awkward situation.

LMC Model, [Social Media Policy](#).

RELEVANT LINKS:

LMC information memo, [Meetings of City Councils](#), Section II-G-8, Telephone, email and social media.

Elected officials should also be mindful of the risks of electronic communication in relation to the Minnesota Government Data Practices Act and the Open Meeting Law. They should consider adopting a policy on electronic communications between councilmembers, and a policy on computer use for elected officials. Remember, two-way communications among elected officials should be strictly avoided due to the possibility of serial meetings in violation of the Open Meeting Law. The Open Meeting Law has been amended to allow for elected officials to post in a social media context with less chance of violating the law. However it's still recommended that elected officials keep issue debate within the confines of a public meeting.

Additional guidelines for elected officials' use of social media include the following:

a. Account names

Personal social media account names should not be tied to the city. This will help clarify that the individual is not speaking officially on behalf of the city. For example, the personal Twitter account for Jane Deer, the Mosquito Heights mayor, should be just "JaneDeer," her Facebook page "Jane Deer's," and so on.

b. Transparency

Elected officials who use personal social media accounts should be encouraged to complete profiles on those sites, and to reveal that they are elected officials for the city. They should be encouraged to include a statement that any opinions they post are their own, not those of the city. They should be aware that—even though they are revealing their affiliation with the city—they will inherently create perceptions about the city among visitors to their personal account sites. Individual actions, whether positive or negative, will impact how the city is viewed. A good rule of thumb to encourage them to follow is that if they would be embarrassed to see their comment appear in the news, they shouldn't post it.

c. Honesty

Encourage elected officials who use personal social media accounts to be honest, straightforward, and respectful. Educate them that if they choose to comment on city issues, they are personally responsible for what they post. They should be mindful of the need to abide by privacy and confidentiality laws in all postings. Officials should be sure that efforts to be honest don't result in sharing non-public information related to colleagues on the council, personnel data, medical information, claims or lawsuits, or other non-public or confidential information.

d. Mistakes, liability, and claims against the city

If an elected official makes a factual mistake, it should be corrected as soon as the official is aware of the error. Corrections should be upfront and as timely as possible. If the elected official is correcting a blog entry, he or she may choose to modify an earlier post, and make it clear the posting has been corrected. If correcting an error in Twitter, the posting might include something designating the corrections, such as “Fixed link” or “Fact correction” before the corrected information.

The web contains a permanent record of mistakes, so attempting to disguise a mistake likely will make things worse.

To help prevent errors, elected officials should not post official information about the city. Potential errors could create city issues ranging from minor to significant, and some may create unforeseen liability issues.

An example discussed earlier in this document applies here. Posting the wrong opening date for enrollment in a parks and recreation program likely will create confusion, inconvenience, and even frustration among residents who try to enroll their kids in a program too early and essentially end up wasting their time, or who find a program full because they tried to enroll their kids too late for a program.

It’s unlikely this type of mistake would create city liability. But posting incorrect information about a new city ordinance related to land use zoning stands a greater chance of creating liability if someone acts based upon that incorrect information, and later is penalized for the action they took based upon the incorrect information officially posted by the city.

If an elected official makes an error related to official city business, he or she should contact the top appointed official to divulge the error and consult on the best manner in which to communicate the correct information. Depending upon the type of error, the city may choose to correct the information in a range of official city communication vehicles such as the city newsletter, website, during a council meeting, and potentially even with the local media to ensure the corrected information is broadcast as widely as possible.

Elected officials also should recognize that using personal technology to communicate on official city business could become inconvenient if a request for data is made on a particular topic, and that elected official has commented through his or her own equipment, including computers and phones.

The official could be in a situation where his or her hard drive is subpoenaed during an investigation of a claim or lawsuit against the city. Such a situation would be inconvenient at best. Elected officials should consider maintaining a separate email from their personal email and consider keeping documents and emails that are city-related separated from their personal information.

RELEVANT LINKS:

e. Add value

There may be times when elected officials use social media to promote a position on a city issue such as a controversial ordinance being considered, to gather feedback from constituents, and/or to campaign. When this occurs, elected officials should be encouraged to add value to the conversation by staying focused on the issue. They should not post comments that amount to name-calling or ridiculing of colleagues, staff, or residents.

While it's common and even natural to seek to respond to attacks on their viewpoints or personality, elected officials should be encouraged to avoid conversations that clearly add no value to discussion of city issues.

For instance, the elected official who essentially is called an "idiot" or some other baited term, should ignore the comment regardless of whether it happens in the social media realm or not, and regardless of who says it. Responding to such comments only serves to inflame discussions, makes all the participants look silly and petty, and casts a long shadow on the view the public has of the city and its elected leaders. Elected officials should seek to elevate conversation, and to be leaders by being respectful, thoughtful, and open-minded.

f. Legal requirements and city policies

Elected officials who use personal social media accounts are not immune from the law, or from the need to follow existing city policies related to electronic communication among councilmembers, and guidelines related to use of city-owned technology. In addition, any information posted or responded to by elected officials should be done so in a manner that does not violate the letter or spirit of the Open Meeting Law. Remember, two-way communications among a quorum of a public body should be strictly avoided due to the possibility of violating the Open Meeting Law—even if the quorum has that discussion between only two members at a time.

Elected officials should be encouraged not to upload, post, transmit, or make available content known to be false, misleading, or fraudulent. They should be encouraged not to post photos that infringe on trademark, copyright, or patent rights of others.

Elected officials never have the right to post non-public and confidential information such as information related to colleagues on the council, personnel data, medical information, claims, or lawsuits against the city.

Elected officials should not use city-owned equipment to post to personal sites content that violates existing city policies, that exhibits hate, bias, discrimination, pornography, libelous, and/or otherwise defamatory content.

[IPAD 09-020](#).

RELEVANT LINKS:

Elected officials should be encouraged to post to personal sites only that content which is suitable for readers and viewers of all ages.

g. Stop comments on city issues

There may be instances in which an elected official should not comment on city issues. This could occur, for example, if the discussion might violate laws, regulations, or confidentiality, or if a claim or lawsuit has been filed against the city.

h. Contact by media

Elected officials who are contacted by the media on a topic of official city business should follow city media relations/communications protocols.