LEAGUE of MINNESOTA CITIES

INFORMATION MEMO

# Computer and Network Loss Control

*Learn about risks in storing and sharing city data on computers and portable devices. Find out how to protect the city from data breaches, virus contamination, ransomware, and hacker attacks. Understand issues with social media such as Facebook, blogs, and Twitter. Links to model employee computer use and social media policies.*

**RELEVANT LINKS:**

See LMC information on *Coverage for Cyber and Computer-Related Risks.*

LMCIT MemberLink forum 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. Doing nothing 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 or floods. Cities insured with the League of Minnesota Cities Insurance Trust (LMCIT) have coverage for a variety of security incident claims, other computer-related liability claims, cyber-caused property damage, cyber crime, and business income/extra expense coverage for property damage claims.

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

## II. Security risks

### A. Physical and electronic security

City data, both public and private, needs to be protected from being accidentally or maliciously deleted. This is similar to paper files. Even if the data is public, you still 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 of your city.

Internal threats include but are not limited to:

- Vendors with inappropriate access.
- Disgruntled employees.
- Untrained employees.
- Former employees whose access has not been removed.

External threats include but are not limited to:

- Vendors.
- Unstable or misleading service providers.
- Hackers.
- Viruses.
- Phishing scams.
- Malware.

Review your internal controls to ensure duties for important or sensitive finance transactions are divided between two or more individuals.

## B. Virus or malware contamination

Contamination of computer systems by viruses or malware is a significant risk. Often, these malicious programs are undetectable without up-to-date antivirus software. Malicious programs can lie dormant for years without actively causing damage.

The types of damage vary. Viruses can destroy city data which can be costly to restore or recreate. Attacks against the city's network may cause slow or unusable network connections. Others may capture keystrokes or passwords for use in other attacks. Viruses may allow hackers to gain unfettered access to a city's network, allowing for data to be read, deleted or, in some cases, encrypted and held hostage for a fee. This is commonly called ransomware and has become an increasing threat to cities.

Viruses replicate and can move from computer to computer via networks, email, flash drives, CDs, DVDs, or even smartphones 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 to attack a 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 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 sue the city for negligence in allowing computers to be so easily commandeered by the hacker.

**RELEVANT LINKS:**

Hackers can monitor and watch the city's communications and then use this information to deceive or manipulate employees into divulging confidential or personal information.

## D. Physical losses

A city may lose data and software from an accident, natural disaster, or other unforeseen 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

Wikipedia, Cloud Computing.

Cloud computing is the "delivery of computing as a service rather than a product." In this model, software applications and information resources are provided to local computers and devices over a network, typically the internet. These "clouds" can be public, private, or a hybrid model.

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 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 can create liability for the city. Misuse can lead to liability from both city employees and third parties. For example, a city employee using city computers to send harassing emails creates liability. Alternatively, an employee may think communications are private, only to find out later that the city was monitoring email. Good guidelines can prevent unintentional misuse and misunderstandings. Comprehensive policies may also limit liability when an incident happens.

Social media is a concern for cities, even if the city does not yet have an official presence on social media, like a Facebook page or Twitter account. Because of the prevalence of social media, instantly accessible through an internet connection, the boundaries between personal and work lives can overlap. For example, an employee's personal social media activity may relate to something that happened at work. Employee's may use social media on city computers and devices.

Ensure your city has clear social media guidelines. Educate employees on how to identify inappropriate content related to city business. Good guidelines are important to keep employees — and the city — out of trouble.

**RELEVANT LINKS:**

## G. Websites and social media information

Material the city posts on its website may open the city to risks, such as the release of private data, or wider harm such as damage to city facilities. For example, if the city pinpoints the location, size, and design of the city's water system facilities or describes its emergency response practices, this information can then be used by bad actors to plan an attack.

Social media platforms are internet and mobile-based tools for sharing and discussing information. While both are 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. When content sign-off isn't required, communications or other guidelines can direct staff in the city's standards and expectations for acceptable and unacceptable website communications. Official social media accounts should also have these safeguards in place.

## H. Demands for data

In either a lawsuit or a data practices request, a demand for information will likely include 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 or other electronic devices may result in employee workers' compensation claims for a repetitive stress syndrome injury. These injuries can result in permanent disabilities, and claims can be expensive.

## J. Staffing

Employees or vendors who maintain the city's network may not have experience with the Minnesota Government Data Practices Act or may not have an appropriate skill set to ensure electronic records are cared for appropriately.

**RELEVANT LINKS:**

Poorly trained information technology staff could unknowingly expose a city's network or computers to security breaches. Poorly vetted staff or vendors could steal or damage equipment, data, or software. Similar to the division of duty often used in a finance office, whenever possible, technology tasks should be divided among staff to ensure more than one person is held accountable and is available.

## K. Portable devices

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

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. The policy should further include cleaning screens on portable devices to ensure that over time, oils from fingertips do not accumulate on the device screen and create a discernable pattern potentially marking the password for that device. Portable device training should 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.

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 data contained on them that is not public.

All computers, including portable devices, should be secured with a strong password or passphrase. 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 portable 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 and portable devices 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 or other internal storage media. It is essential that the storage media be 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 include:

- Copiers/scanners
- Fax machines
- Computers
- Cameras
- Portable devices (USB flash drives, phones, tablets, laptops, 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.

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. Whenever possible, grant access with minimal capabilities. For example, some users need rights to only read data. Control closely who needs access to move, write, or delete 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 always have their own unique 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. Complex passwords or passphrases include spaces, numbers, special characters, and other symbols.

**RELEVANT LINKS:**

Shared and administrative passwords should be changed, at the minimum, annually, or when an employee or vendor who has access to the password has an employment change. It is very important to change system default account names and the corresponding passwords to unique and complex passwords or passphrases. Default settings for account names and passwords are often used by monitoring or other equipment connected to the internet (often referred to as the Internet of Things, or IoT). Using default account names and passwords is a security risk because that information is published in the equipment instruction manuals.

See, Wikipedia, Social Engineering (Security) for current examples of social engineering.

City staff and elected officials are also key to computer security. Social engineering — 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. Antivirus software

Ensure all devices used for city business (including devices at home if used to do city work) have current, updated antivirus software installed. There are many vendors that offer antivirus 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" antivirus 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.

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, individual 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).

**RELEVANT LINKS:**

For additional information about encryption see Wikipedia, Encryption.

## D. Data encryption

While the majority of city data is 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 becoming best practice to encrypt server data. While less critical than securing end-user devices, it's another layer of protection for city data.

External connections, such as a VPN, cloud services, 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 compromised by hackers. City staff should be trained to not transmit private data over wireless networks.

## F. Cloud computing

Before storing any city data in a cloud-based application, it is paramount to first 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 retrieve the data. This is especially important for how the data is backed up. In some 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.

Most reputable technology vendors require background checks and, upon request, will provide documentation that they performed the check. Using a high school student or relative of a city official is 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.

**RELEVANT LINKS:**

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 the process of creating data connections (mappings) between two distinct data components. Mapping assists in understanding the relationship between different data. It is critical to keeping a network organized and reducing costs of e-discovery and data practices requests. 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 different folder where only city staff tasked with HR responsibilities can access it. Less sensitive data could then be stored in a separate folder with less restrictive access.

Whenever possible, grant access with minimal capabilities. For example, some users need rights to only read data. Closely control who needs access to move, write, or delete data. 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.

Minn. Stat. § 13.05, subd. 5.
Minnesota Department of Administration Data Practices Office sample *Policy for Ensuring the Security of Not Public Data.*

Minn. Stat. § 13.055, subd. 1-6.

Minn. Stat. § 13.09.

By law, cities must establish security measures to help ensure that non-public 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 the event of a breach, cities must conform with the disclosure and notice statutes regarding the breach. Accessing non-public data without authorization is a misdemeanor. 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, antivirus 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 to protect city data from natural disaster, failed hardware, viruses, or hacker attacks. Cities need a plan in the event that the device performing the backups is damaged or out of order. 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 daily. 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.

Address how email, and backups containing email, are handled in the city's records retention schedule. Cities should backup email separately so that it is not retained indefinitely along with other city data requiring longer retention. A separate email backup also ensures archived electronic city records do not need to be searched as part of a discovery or data practices request.

## K. Computer use and social media policies

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.

Adopt a computer use policy and ensure all staff members are aware of the policy. Make sure the policy includes the use of social media for personal and professional purposes. Decide whether the city has an official presence on social media platforms. If so, decide whether the city will adopt a centralized or decentralized strategy for interacting on social media platforms. Make sure city employees are aware of the policy and consistently enforce it. Consider voluntary policy language to govern elected officials' use of city-owned technology, social media, and other electronic communications.

## L. Website and social media policies

**RELEVANT LINKS:**

*Computer Use*, LMC Model Policy.

*Social Media*, LMC Model Policy.

Think about the kind of information posted on the city's website. Make sure that private data is not posted. Public data should be accurate and accessible, according to the Americans with Disabilities Act (ADA). 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 is largely 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

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

**RELEVANT LINKS:**

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. On social media platforms, 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.

*Davison v. Randall*, 912 F.3d 666 (4th Cir. 2019).

When Cities engage in two-way communication, there are First Amendment concerns. Cities should never take an action to curtail speech based on viewpoint. Cities are encouraged to work with the city attorney, and perhaps start with the League's sample social media policy, to carefully moderate comments by the public for the benefit of all.

## 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. Microblogs are 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 Twitter, Instagram or 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.

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. Different tools work well for different types of information.

### (1) Microblogs

Microblogs such as Twitter or Instagram 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.

### (3) Video sites

Video sites, such as YouTube, Vimeo, and Facebook Live, 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. Consider video sites that offer closed captioning or other accessibility options.

### (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 way 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.

**RELEVANT LINKS:**

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.

### 3. Records retention

Handbook, *Records Management*.

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

*Computer Use,* LMC Model Policy.

*Social Media*, LMC Model 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.

**RELEVANT LINKS:**

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.
- 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.
- Outline appropriate locations to store city electronic data.

## A. Human resources concerns

There are many areas of overlap between computer use policies and human resources polices. 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 security vulnerabilities into the city's computer system, but many 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 to remind employees about the policy you've put in place.

**RELEVANT LINKS:**

## 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?

## 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

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

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 document the inventory, communicate expectations, and limitations about how that equipment is used.

# B. Technology concerns

Because technology and technology risks change 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 an annual review and employee signoff.

**RELEVANT LINKS:**

## 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.
- Whether or not staff or elected officials are required to use city email accounts.
- 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 and report "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, are allowed. If allowed, outline the steps to take before using this type of technology.
- Standards for encrypting confidential data in email or 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. Your city is probably operating a specific kind of antivirus 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.

**RELEVANT LINKS:**

*Computer Use,* LMC Model Policy.

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:

**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 antivirus 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 or mp4 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 backups of city email and how long you will retain those backups. It's recommended to back up email systems separately from all other system backups.
- Whether you will provide or permit any communication by instant messaging (IM) and, if so, what product.
- 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:**

# C. Social media

## 1. Included or not

*Social Media*, LMC Model Policy.

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.

*Social Media and Digital Images*, LMC Model Policy for Fire Departments and Emergency Medical Services.

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 should be dedicated to communicating information 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.

For purposes of managing government data created in social media, the city should maintain a list of social media accounts the city has created and controls. These may include city-owned accounts for use by elected officials, but the city shouldn't claim to control or own accounts that it does not create or cannot access.

See DPO 19-001.

The city should determine whether it wants 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 strategies 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 and access to the system documented in the event a backup person is needed. 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.

**RELEVANT LINKS:**

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.

General Records Retention Schedule for MN Cities (see PDF page 27).

Records retention and data practices requests can be easy for most cities when it comes to social media. For those cities following the state records retention schedule, social media messages considered "incidental and non-vital correspondence" need only be retained "until read." In essence, under the state schedule, the city that does not use social media for "transactions of city business" need not retain any social media data, thus making data requests related to it easier. For city postings that arguably "relate to transactions of city business," it might make sense to retain copies of those in a separate file so that it is easy to produce should there be a request made under the state Data Practices Act.

Etiquette guidelines may help set expectations. This section illustrates some possible guidelines a city may consider incorporating into their social media policy.

## a. Account names

General social media pages, such as Facebook pages should clearly indicate they are tied and monitored by 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 its 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, 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. The web contains a permanent record of mistakes, so attempting to disguise a mistake likely will make things worse.

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.

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 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.

**RELEVANT LINKS:**

## e. Legal requirements and city policies

*Davison v. Randall*, 912 F.3d 666 (4th Cir. 2019).

Although the legal landscape for social media is still developing, there are clear First Amendment considerations for social media use by the city and its officials. Cities and their officials should generally not "block" or "ban" private citizens on social media platforms, and never merely on the basis of the content of the message. And because the city's social media account likely creates a "public forum," there are limited circumstances under which comments by the public should be removed. Cities are encouraged to work with the city attorney, and perhaps start with the League's sample social media policy, to carefully moderate comments by the public for the benefit of all.

*Social Media*, LMC Model Policy.
*Social Media and Digital Images*, LMC Model Policy for Fire Departments and Emergency Medical Services.

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.
- Never share non-public and confidential information such as information related to co-workers, personnel data, medical information, claims, or lawsuits against the city. 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 exhibit 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 maintaining 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.
- 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 or tags to other social media posts when it is relevant to the city.

**RELEVANT LINKS:**

## g. Media contact

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

## 3. City staff personal use

*Social Media*, LMC Model Policy.

*Social Media and Digital Images*, LMC Model Policy for Fire Departments and Emergency Medical Services.

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 (APWA). 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.

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

**RELEVANT LINKS:**

For more information about Employee's right to speak publicly, see Government as Employer: Freedom of Speech from the Legal Information Institute.

## a. Employee right to speak publicly

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, is 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 not post content that infringes 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.

## 4. Elected officials' social media use

See Minn. Stat. § 211B.09.

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.

*Davison v. Randall*, 912 F.3d 666 (4th Cir. 2019).

Elected officials should be mindful of whether their social media account is — or appears to be — an account for their official capacity or a personal account. If an elected official has a private social media account, but "clothes it in the power and prestige" of his or her office, the account may be deemed a government account and perhaps even a "public forum" from which people may not be excluded, blocked, or muted.

**RELEVANT LINKS:**

See DPO 19-001.

One solution is for elected officials to use city-owned social media accounts for communications related to their office, and to leave any official capacity out of any private account communications. The city's social media policy can aid in this by specifying city social media accounts it considers "official" and therefore creating "government data." This will help clarify how a city may respond when asked for information on a given account.

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 information memo, *Meetings of City Councils*, Section II-G-8, Telephone, email and social media.
Minn. Stat. 13D.065.

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 council members, 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 and the city may be legally responsible for what they post. Elected official 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. The web contains a permanent record of mistakes, so attempting to disguise a mistake likely will make things worse.

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 on Twitter, the posting might include something designating the corrections, such as "Fixed link" or "Fact correction" before the corrected information.

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, but incorrect information about a new city ordinance related to land use zoning could create legal liability if someone acts on the incorrect information, and is penalized when they act on that incorrect information.

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 way 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.

**RELEVANT LINKS:**

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 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.

## 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 social media accounts in their official capacity are not immune from the law, or from the need to follow existing city policies related to electronic communication among council members, 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.

DPO 09-020.

**RELEVANT LINKS:**

Elected officials should be encouraged not to upload, post, transmit, or make available content known to be false, misleading, or fraudulent. They should not post content that infringes 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.

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

*Davison v. Randall*, 912 F.3d 666 (4th Cir. 2019).

Finally, elected officials should never block or ban someone following their social media presence simply on the basis of their viewpoint or the content of a message. Elected officials are encouraged to work with the city attorney to carefully moderate comments by the public for the benefit of all.

## 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.

**RELEVANT LINKS:**

## Cases



## Statutes



## Reference



## DPO



## Document Reference



## Information Memo



## LMC Reference



## Handbook