CITY OF TONKA BAY
ITEM NO. 9B

Memo

To: Honorable Mayor and City Council

From: Joe Kohlmann, City Administrator

Date: January 27, 2015

Re: Computer Use Policy

Staff has located the *attached computer use policy* and *informational Memo* from the League of Minnesota Cities. The Computer Use Policy seems to comprehensively address computer use. This includes: personal use, hardware, software, email, calendars, instant messaging, personal devices, and security- which all apply to Tonka Bay's situation.

Staff sees the City's computer use issues broken down in two different areas – **email and the device itself**.

EMAIL

Staff was quoted to $50 per email address for an @cityoftonkabay.net email address. Along with this, there would likely be IT costs to convert the "webmail" into a more user friendly email interface – such as outlook, gmail, yahoo, etc. Basically, forwarders from the webmail would be used to go from webmail to a more user friendly email service.

To date, Councilmembers have been using their personal email addresses. If a data request were to be submitted, personal emails would need to be scanned for City applicable emails. To avoid future cost and comingling of personal, business and City emails – Staff would recommend Councilmembers set up a free email through gmail that they conduct their City business on.

Device

The League Computer Use Policy outlines what a policy may look like- regulating internet, searches, software, personal use, hardware, calendars, etc. This creates some issues. First, the City is moving into the electronic age with electronic transmission of documents, files, communications, etc. As Councilmembers, you will be required to use an electronic device to conduct City

business. Second, each councilmember likely has different electronic devices (phone, computer, laptop, etc.) for their business and personal electronic use. So essentially, the City is adding a second, third, or fourth device for Councilmembers to be responsible for. Also, some Councilmembers may wish to use the issued device on different programs, such as word, excel, etc. The City would then be in the position of regulating/purchasing/monitoring software for the devices.

The electronic device issued from the City should make things easier on Councilmembers and it is less expensive for the City. It also enables Staff to reach Councilmembers on an electronic device that they should have with them to a reasonable degree. The cost of the ipad was approximately $500. Councilmembers, over a four year term, they participate in at least 92 meetings. The cost per meeting is about $5.43 for the ipad. In addition, with technological advances, there is no saying that the device used today, is the device the City will want to use in four years.

Staff thinks that Councilmembers should be provided the advance toward the device that they will own. They can then use the computer device for their personal, business, and City use. The gmail address would be the "buffer" for any communications for City business. If there were a data request, then the gmail account is realistically the only applicable database to be searched, not the device itself.

Also, Councilmembers can then integrate their device with personal and business use to have a centralized device and be available.

Staff recommends a reimbursement to account for the cost of this. As stated above, the reimbursement is approximately $5.43 per meeting- to offset costs associated with being a Councilmember (i.e. the requirement of an electronic device to process City business). Some City Staff members currently receive a reimbursement for cell phone usage. So the Staff members own their phone but some of the costs associated with the requirement of having a phone are provided. This would be a similar concept.

This seems to be the best option in protecting Councilmembers personal/business information; removing the City from liability/monitoring of the devices; and allowing the City to move forward with technological advances.

Attached is a sample Computer Use Policy from the League
Attached is an excerpt from a League Memo regarding electronic devices.

Council Action Requested:
Review and discuss.

Model Computer Use Policy

Before adopting this policy, a city should be familiar with the contents of the LMC information memo, *Computer and Network Loss Control*. This model policy assigns duties to certain departments and staff titles. Suggestions are offered in parentheses. Use departments and staff positions that are appropriate for your city. You may modify other provisions to conform to your city's situation as needed.

This model contains a number of provisions with legal implications. Before adopting a city policy based on this model, please review it with your city attorney.

City of _____ Computer Use Policy

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

Computers and related equipment used by City employees are property of the City. The City reserves the right to inspect, without notice, all data, emails, files, settings, or any other aspect of a City-owned computer or related system, including personal information created or maintained by an employee. The City may conduct inspections on an as-needed basis as determined by _____ (City Administrator/Manager/Council/ or Other Designee).

Beyond this policy, the _____ (Information Technology or other appropriate department or position) may distribute information regarding precautions and actions needed to protect City systems; all employees are responsible for reading and following the guidance and directives in these communications.

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

Reasonable, incidental personal use of City computers and software (e.g., word processing, spreadsheets, email, Internet, etc.) is allowed but should never preempt or interfere with work. All use of City computers and software, including personal use, must adhere to provisions in this policy, including the following:

- Employees shall not connect personal peripheral tools or equipment (such as printers, digital cameras, disks, USB drives, or flash cards) to City-owned systems, without prior approval from the _____ (Information Technology Director or his/her designee, or another position you may name). If permission to connect these tools/peripherals is granted, the employee must follow provided directions for protecting the City's computer network.

- Personal files should not be stored on City computer equipment. This also applies to personal media files, including but not limited to mp3 files, wav files, movie files, iTunes files, or any other file created by copying a music CD, DVD, or files from the Internet. _____ (Information Technology, or alternate positions you may name) staff will delete these types of files if found on the network, computers, or other City-owned equipment. Exceptions would be recordings for which the City has created, owns, purchased, or has a license.
- City equipment or technology shall not be used for personal business interests, for-profit ventures, political activities, or other uses deemed by the _____ (City Administrator/Manager/Council or other designee) to be inconsistent with City activities. If there is any question about whether a use is appropriate, it should be forwarded to _____ (Human Resources, or your personnel staff) for a determination.

Hardware

In general, the City will provide the hardware required for an employee to perform his or her job duties. Requests for new or different equipment should be made to your supervisor, who will forward the request to _____ (Information Technology, or other department or staff with this responsibility).

The City will not supply laptop computers based solely on the desire of employees to work offsite. A laptop request form will be required for each laptop deployment, and must be signed off by the employee's supervisor and department head. Laptops will only be issued to employees who: travel frequently and require the use of a full computer while traveling; regularly use their laptop offsite; require a laptop for access to special software or systems; and/or have a documented business need for a laptop.

Only City staff may use City computer equipment. Use of City equipment by family members, friends, or others is prohibited.

Employees are responsible for the proper use and care of City-owned computer equipment. City computer equipment must be secured while off City premises; do not leave computer equipment in an unlocked vehicle or unattended at any offsite facility. Computer equipment should not be exposed to extreme temperature or humidity. If a computer is exposed to extreme heat, cold, or humidity, it should be allowed to achieve normal room temperature and humidity before being turned on.

Software

In general, the City will provide the software required for an employee to perform his or her job duties. Requests for new or different software should be made to your supervisor, who will forward the request to _____ (Information Technology, or other department or staff with this responsibility).

Employees shall not download or install any software on their computer without the prior approval of the _____ (Information Technology Director, or other staff in your city with this authority). Exceptions to this include updates to software approved by

Information Technology such as Microsoft updates, Adobe Reader, and Adobe Flash. _____ (Information Technology, or another department or staff member you name) may, without notice, remove any unauthorized programs or software, equipment, downloads, or other resources.

Electronic Mail: The City provides employees with an email address for work-related use. Some personal use of the City email system by employees is allowed, provided it does not interfere with an employee's work and is consistent with all City policies.

Employee emails (including those that are personal in nature) may be considered public data for both e-discovery and information requests and may not be protected by privacy laws. Email may also be monitored as directed by the City authorized staff and without notice to the employee.

Employees must adhere to these email guidelines:

- Never transmit an email that you would not want your supervisor, other employees, members, city officials, or the media to read or publish (e.g., avoid gossip, personal information, swearing, etc.).
- Use caution or avoid corresponding by email on confidential communications (e.g., letters of reprimand, correspondence with attorneys, medical information).
- Do not open email attachments or links from an unknown sender. Delete junk or "spam" email without opening it if possible. Do not respond to unknown senders.
- Do not use harassing language (including sexually harassing language) or any other remarks, including insensitive language or derogatory, offensive, or insulting comments or jokes.

Electronic Calendars: A shared calendar environment is provided as part of the City's email software program. All employees are required to keep their electronic calendar up to date and, at a minimum, must grant all staff the ability to view their calendar.

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

Personal Devices: Employees may choose to use their own equipment to read or compose email or other City data as governed in this policy. Employees understand that by connecting their personal equipment to the City's email server, their personal devices could be searched during an e-discovery or other court-ordered scenarios, and agree to grant access to their personal devices should such a situation arise.

Security

Passwords: Employees are responsible for maintaining computer/network passwords and must adhere to these guidelines:

- Passwords must be at least eight characters long and include at least three of the following: lowercase character; uppercase character; and a number or non-alpha-numeric character (e.g., *, &, %, etc.). (Example: J0yfu11y!) Password requirements may be changed as necessary, as determined by the _____ (Information Technology Director, or other staff member you may name).
- Passwords should not be shared or told to other staff. If it is necessary to access an employee's computer when he or she is absent, contact your supervisor or the _____ (HR Director, or other staff charged with personnel duties); _____ (Information Technology, or other staff you may designate) will not provide access to staff accounts without approval of the _____ (department director, HR Director, or another staff member the city may designate).
- Passwords should not be stored in any location on or near the computer, or stored electronically such as in a cell phone or other mobile device.
- Employees must change passwords every 60 days when prompted, or on another schedule as determined by the _____ (Information Technology Director, or other staff title charged with technology responsibilities).

Network access: Non-City-owned computer equipment used in the City's building should only use the wireless connection to the Internet. Under no circumstances should any non-City-owned equipment be connected to the City's computer network via a network cable. Exceptions may be granted by _____ (a member of the Information Technology team, or other staff title charged with technology responsibilities).

Personal computer equipment may not be connected to the City's network without prior approval of the _____ (Information Technology Director or his/her designee, or other staff title charged with technology responsibility). Personal equipment may be subject to password requirements or other electronic security measures as determined by the _____ (Information Technology Director, or other staff to whom you assign this responsibility).

Remote Access to the Network: Examples of remote access include, but are not limited to: Outlook Web Access (web mail), virtual private network (VPN), Windows Remote Desktop, and Windows Terminal Server connections. While connected to City computer resources remotely, all aspects of the City's Computer Use Policy will apply, including the following:

- With the exception of Outlook Web Access, remote access to the City's network requires a request from a supervisor and approval from the _____ (Director of Information Technology or other staff member you assign to this responsibility). Remote access privileges may be revoked at any time by an employee's _____ (supervisor, Human Resources in conjunction with the Director of Information Technology Services, or other staff with similar responsibilities in your city).
- If remote access is from a non-City-owned computer, updated anti-virus software must be installed and operational on the computer equipment, and all critical operating system updates must be installed prior to connecting to the City network remotely. Failure to comply could result in the termination of remote access privileges.

- Recreational use of remote connections to the City's network is strictly forbidden. An example of this would be a family member utilizing the City's cellular connection to visit websites.
- Private or confidential data should not be transmitted over an unsecured wireless connection. Wireless connections are not secure and could pose a security risk if used to transmit City passwords or private data while connecting to City resources. Wireless connections include those over cellular networks and wireless access points, regardless of the technology used to connect.

Internet

The following considerations apply to all uses of the Internet:

- Information found on the Internet and used for City work must be verified to be accurate and factually correct.
- Reasonable personal use of the Internet is permitted. Employees may not at any time access inappropriate sites. Some examples of inappropriate sites include but are not limited to adult entertainment, sexually explicit material, or material advocating intolerance of other people, races, or religions. If you are unsure whether a site may include inappropriate information, you should not visit it.
- If an employee's use of the Internet is compromising the integrity of the City's network, _____ (Information Technology) staff may temporarily restrict that employee's access to the Internet. If _____ (Information Technology) staff does restrict access, they will notify the employee, HR, and the employee's manager as soon as possible, and work with the employee and manager to rectify the situation.
- The City may monitor or restrict any employee's use of the Internet without prior notice, as deemed appropriate by the employee's _____ (manager in consultation with the HR Director and the City Administrator/Manager/Council/other).

Data Retention

Electronic data should be stored and retained in accordance with the City's records retention schedule.

Storing and Transferring Files: If you are unsure whether an email or other file is a government record for purposes of records retention laws or whether it is considered protected or private, check with your supervisor. If you are unsure how to create an appropriate file structure for saving and storing electronic information, contact the _____ (Information Technology Department, or other department or staff member you may designate).

Employees must adhere to these guidelines when transferring and storing electronic files:

- All electronic files must be stored on network drives. The City will not back up documents stored on local computer hard drives, and holds no responsibility for recovery of documents on local computer hard drives should they fail. Files may be temporarily stored on a laptop hard drive when an employee is traveling/offsite; however, the files should be copied to network as soon as possible.
- Electronic files, including emails and business-related materials created on an employee's home or personal computer for City business, must be transferred to and

stored on the City's network. City-related files should not be stored on an employee's personal computer, unless otherwise defined in this policy.

- All removable storage media (e.g., CD-ROM, flash or USB drive, or other storage media) must be verified to be virus-free before being connected to City equipment.
- Email that constitutes an official record of City business must be kept in accordance with all records retention requirements for the department and should be copied to the network for storage.
- Email that is simple correspondence and not an official record of City business should be deleted (from both the "Inbox" and the "Deleted" box) as soon as possible and should not be retained by employees for more than three months. The City will not retain emails longer than one year on the network or in network back-ups.
- Electronic files or emails that may be classified as protected or private information should be stored in a location on the City's network that is properly secured.
- Any files considered private or confidential should not be stored anywhere other than the City's network. If there is a need to take confidential information offsite, it must be stored on encrypted media; _____ (Information Technology or other staff you may name) can assist in the encryption of media.

Employee signature

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

_____ (Print Employee Name)

_____ (Employee Signature)

_____ (Print Department Name)

_____ (Date)

RELEVANT LINKS:

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, *Electronic Communications Between Council Members.*

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.
- 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

RELEVANT LINKS:

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.

See LMC Model Computer Use 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:

- 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.

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.

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.

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.

RELEVANT LINKS:

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. 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.

RELEVANT LINKS:

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.
- 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. 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:

(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.

RELEVANT LINKS:

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 information memo, *Electronic Communications Between Council Members.*

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.

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 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.

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 elected officials should be strictly avoided due to the possibility of serial meetings in violation of the Open Meeting Law.

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.