CITY OF BIG LAKE

COMPUTER USE

SOCIAL MEDIA

CITY ISSUE DEVICES

POLICIES

Adopted by Big Lake City Council – May 24, 2017

Contents

COMPUTER USE

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 or Council.

Beyond this policy, the City Administrator or City Clerk 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:

- 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 or Council to be inconsistent with City activities. If there is any question about whether a use is appropriate, it should be forwarded to City Administrator 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 the City Administrator.

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 City Administrator.

Employees shall not download or install any software on their computer without the prior approval of the Department Director and/or City Administrator. Exceptions to this include updates to software approved by Information Technology consultant such as Microsoft updates, Adobe Reader, and Adobe Flash. The City Administrator or Department Director may, without notice, direct the Information Technology consultant to 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, if there is a purpose grant staff the ability to view their calendar.

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:

- Password requirements may be changed as necessary, as determined by the Information Technology consultant, City Clerk and/or City Administrator.
- 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 City Administrator; Information Technology consultant or City Clerk will not provide access to staff accounts without approval of the Department Director or City Administrator.
- 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 consultant, City Clerk and/or City Administrator.

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 the City Administrator.

Personal computer equipment may not be connected to the City's network without prior approval of the City Administrator. Personal equipment may be subject to password requirements or other electronic security measures as determined by the Information Technology consultant and City Administrator.

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 City Administrator. Remote access privileges may be revoked at any time by an employee's supervisor or the City Administrator.
- 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 consultant staff may temporarily restrict that employee's access to the Internet. If Information Technology consultant staff does restrict access, they will notify the employee, the City Administrator, the City Clerk, 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 supervisor and/or the City Administrator.

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 City Clerk.
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 consultant, City Clerk or City Administrator can assist in the encryption of media.

SOCIAL MEDIA

Purpose

Social networking in government serves two primary functions: to communicate and deliver messages directly to citizens and to encourage citizen involvement, interaction, and feedback. Information which is distributed via social networking must be accurate, consistent, and timely and meet the information needs of the City's customers. Since social media is used for social networking, this policy seeks to ensure proper use of the City of Big Lake's social media sites by its representatives.

The City of Big Lake wishes to establish a positive and informative social media presence. City representatives have the responsibility to use the City's social media resources in an efficient, effective, ethical and lawful manner pursuant to all existing City and departmental policies. This policy also provides guidelines and standards for city representatives regarding the use of social media for communication with residents, colleagues and all other followers.

Policy

The City of Big Lake will determine, at its discretion, how its web-based social media resources will be designed, implemented and managed as part of its overall communication and information sharing strategy. City social media sites may be modified or removed by the City at any time and without notice, as described in this document.

City of Big Lake social media accounts are considered a City asset and administrator access to these accounts must be securely administered in accordance with the City's Computer Use policy. The City reserves the right to shut down any of its social media sites or accounts for any reason without notice.

All social media web sites created and utilized during the course and scope of an employee's performance of his/her job duties will be identified as belonging to the City of Big Lake, including a link to the City's official web site.

Scope

This policy applies to any existing or proposed social media web sites sponsored, established, registered or authorized by the City of Big Lake. This policy also covers the private use of the City's social media accounts by all City representatives, including its employees and agents, Council members, appointed board or commission members and all public safety volunteers to the extent it affects the City. Questions regarding the scope of this policy should be directed to the City Administrator.

Definition

Social media are internet and mobile-based applications, websites and functions, other than email, for sharing and discussing information, where users can post photos, video, comments and links to other information to create content on any imaginable topic. This may be referred to as "user-generated content" or "consumer-generated media."

Social media includes, but is not limited to:

- Social networking sites such as Facebook, LinkedIn, Twitter, and online dating services/mobile apps
- Blogs
- Social news sites such as Reddit and Buzzfeed
- Video and photo sharing sites such as YouTube, Instagram, SnapChat, and Flickr
- Wikis, or shared encyclopedias such as Wikipedia
- An ever emerging list of new web-based platforms generally regarded as social media or having many of the same functions as those listed above

As used in this policy, "employees and agents" means all City representatives, including its employees and other agents of the city, such as independent contractors or Council members.

Rules of Use

City employees and agents with administrator access are responsible for managing social media websites. Facilities or departments wishing to have a new social media presence must initially submit a request to the City Administrator or designee in order to ensure social media accounts are kept to a sustainable number and policies are followed. All approved sites will be clearly marked as the City of Big Lake site and will be linked with the official City website (www.biglakemn.org). No one may establish social media accounts or websites on behalf of the City unless authorized in accordance with this policy

Administration of all social media web sites must comply with applicable laws, regulations, and policies as well as proper business etiquette.

City social media accounts accessed and utilized during the course and scope of an employee's performance of his/her job duties may not be used for private or personal purposes or for the purpose of expressing private or personal views on personal, political or policy issues or to express personal views or concerns pertaining to City employment relations matters.

No social media website may be used by the City or any City employee or agent to disclose private or confidential information. No social media web site should be used to disclose sensitive information; if there is any question as to whether information is private, confidential or sensitive, contact the City Administrator.

When using social media sites as a representative of the City, employees and agents will act in a professional manner. Examples include but are not limited to:

- Adhere to all City personnel and Computer Use policies
- Use only appropriate language

Be aware that content will not only reflect on the writer but also on the City of Big Lake as a whole, including elected officials and other city employees and agents. Make sure information is accurate and free of grammatical errors.

- Not providing private or confidential information, including names, or using such material as part of any content added to a site.

- Not negatively commenting on community partners or their services, or using such material as part of any content added to a site.
- Not providing information related to pending decisions that would compromise negotiations.
- Be aware that all content added to a site is subject to open records/right to know laws and discovery in legal cases.
- Always keep in mind the appropriateness of content.
- Comply with any existing code of ethical behavior established by the City.

Where moderation of comments is an available option, comments from the public will be moderated by City staff, with administrative rights, before posting. Where moderation prior to posting is not an option, sites will be regularly monitored by City staff.

City of Big Lake's staff with administrative rights will not edit any posted comments. However, comments posted by members of the public will be removed if they are abusive, obscene, defamatory, in violation of the copyright, trademark right or other intellectual property right of any third party, or otherwise inappropriate or incorrect. The following are examples of content that may be removed by City staff before or shortly after being published:

- Potentially libelous comments
- Obscene or racist comments
- Personal attacks, insults, or threatening language
- Plagiarized material
- Private, personal information published without consent
- Comments totally unrelated to the topic of the forum
- Commercial promotions or spam
- Hyperlinks to material that is not directly related to the discussion

Personal Social Media Use

The City of Big Lake respects employees and agents' rights to post and maintain personal websites, blogs and social media pages and to use and enjoy social media on their own personal devices during non-work hours. The City requires employees and agents to act in a prudent manner with regard to website and internet postings that reference the City of Big Lake, its personnel, its operation or its property. Employees and agents and others affiliated with the City may not use a city brand, logo or other city identifiers on their personal sites, nor post information that purports to be the position of the City without prior authorization.

City employees and agents are discouraged from identifying themselves as city employees when responding to or commenting on blogs with personal opinions or views. If an employee chooses to identify him or herself as a City of Big Lake employee, and posts a statement on a matter related to City business, a disclaimer similar to the following must be used:

> "These are my own opinions and do not represent those of the City."

Occasional access to personal social media websites during work hours is permitted, but employees and agents must adhere to the guidelines outlined in the City's Computer Use policy

and the City's Respectful Workplace policy. Employees and agents should also review the Ownership section of this policy (below).

There may be times when personal use of social media (even if it is off-duty or using the employee's own equipment) may spill over into the workplace and become the basis for employee coaching or discipline. Examples of situations where this might occur include:

- Friendships, dating or romance between co-workers
- Cyber-bullying, stalking or harassment
- Release of confidential or private data; if there are questions about what constitute confidential or private data, contact the City Administrator.
- Unlawful activities
- Misuse of city-owned social media
- Inappropriate use of the city's name, logo or the employee's position or title
- Using city-owned equipment or city-time for extensive personal social media use

Each situation will be evaluated on a case-by-case basis because the laws in this area are complex. If you have any questions about what types of activities might result in discipline, please discuss the type of usage with the City Administrator.

Data Ownership

All social media communications or messages composed, sent, or received on city equipment in an official capacity are the property of the City and will be subject to the Minnesota Government Data Practices Act. This law classifies certain information as available to the public upon request. The City of Big Lake also maintains the sole property rights to any image, video or audio captured while a City employee is representing the City in any capacity.

The City retains the right to monitor employee's social media use on city equipment and will exercise its right as necessary. Users should have no expectation of privacy. Social media is not a secure means of communication.

Policy Violations

Violations of the Policy will subject the employee to disciplinary action up to and including discharge from employment.

CITY ISSUED DEVICE GUIDELINES

General Information

These guidelines pertain to city employees, elected and appointed officials who are issued a device purchased by the city. The purpose of these guidelines is to outline the responsibilities and care required for the city-issued devices.

The devices are intended to be utilized by staff members and elected and appointed officials for the purpose of enhancing meeting workflow, reducing the use of paper agenda packet materials, improve staff efficiency, and to improve the timeliness of Council, staff and resident communication.

City Use

Issued devices are intended for professional use. The city does not maintain loaner devices, so users will be responsible for conducting meetings without a device in the event of a lost or misplaced device.

- Devices shall be maintained in a suitable charged state during work hours.
- Inappropriate media may not be used as a screensaver or background photo.
- Devices will be secured with a password.
- Sound shall be muted at all times unless needed for instructional purpose.
- Personally owned music, games and apps may only be present on city-issued device when using a personal account.
- In case a device is restored to its original condition, the user is responsible for restoring any personal content.
- City staff is not responsible for backing up personal related content.
- Users may save work locally on the device. It is strongly recommended that users utilize the city-designated online storage technology.
- Information stored on a city own device could be classified as public, private, or other data and is governed by Minnesota Government Data Practice Act (MN Statute Chapter 13) and must be treated accordingly.
- Staff, elected or appointed officials should retain information stored on any city-issued device in keeping with city policies and procedures per the General Records Retention Schedule.

Personal/Home Use

City-issued devices may be taken home provided the use is consistent with the Electronic Media Usage Policy portion found in the Personnel Policy Manual and the City Computer Use Policy. Failure to adhere to the policy shall result in the revocation of such use privilege.

- Users are allowed to connect devices to non-city wireless networks.
- While instruction and advice may be offered, city staff is not responsible for home network use or support.
- It is the policy of the city to maintain the right to access and disclose any and all message communicated through electronic means when city-issued equipment is used. Regardless of the intent of the message (business or personal), any employee and/or city official involved has no right to privacy, or to the expectation of privacy,

concerning the content of any message or the intended destination of any message when using city-issued equipment.

Device Care

User will be held responsible for the maintenance and care of assigned communication devices.

- Keep batteries charged and ready for use at meetings.
- Clean the view screen with a soft, dry cloth or anti-static cloth as needed.
- Do not lean or place anything on the screen that may cause damage.
- Utilize the protective case at all times.
- When not in use, store in a secure location. Never leave in an unlocked care or any other theft-prone area.
- Immediately report lost stolen, malfunctioning or damage devices to the City Clerk.
- Stolen devices must be reported immediately to the local authorities.
- Consult with the City Clerk office before connecting or syncing devices to another computer.
- Upon request, devices must be delivered to the City Clerk's office for annual maintenance.

Application Software

All software applications purchased and installed by the city staff must remain on the device in a usable condition and be accessible at all times. Users are responsible for personal software applications and are responsible for installation and backup.

- Software purchased by the city will be coordinated through the city IT consultant.
- Users are allowed to purchase and download personal applications providing they are not profane, obscene or offensive to others. The city reserves the right to remove any personal applications at any time for any reason.
- The city is not responsible for the loss of any personal software applications when they device is updated, tested with diagnostic tools or restored to its original state.
- Storage space needed for city applications will take precedence over space used for personal items.

COMPUTER – SOCIAL MEDIA – CITY DEVICES POLICIES ADOPTION

The Computer/Social Media/City Issued Device Policies shall be adopted by the City Council. The policies shall be reviewed by the Finance Department staff on an ongoing basis and any modifications made thereto must be approved by the City Council.

Adopted by City Council May 24, 2017

Revisions: