CITY OF PRINCETON, MINNESOTA
COMPUTER USE POLICY

General Information

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

Computers and related equipment used by City employees are the property of the City. This property includes, but is not limited to, hardware, software, email messages, data files and voicemail. 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 the City Administrator.

Beyond this policy, the City's Technology Services Manager 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.

Inappropriate Use of City Technology

Employees should not use City technology for any purpose that could reflect negatively on the City. The following is a list of inappropriate uses of the City's technology which may result in disciplinary action up to and including a dismissal. This is not a complete list of inappropriate uses. If an employee does not know whether a particular use would be allowed under this policy, they should check with their supervisor or the Technology Services Manager.

- Displaying, printing, or transmitting material that contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material.
- Displaying, printing, or transmitting material that violates City regulations prohibiting sexual harassment.
- Using the City's computer system or software or allowing others to use it for personal profit, commercial product advertisement, or partisan political purposes.
- Using e-mail to solicit for commercial ventures, or charitable, religious, or political causes, with the exception of charitable campaign drives sponsored by the City.
- Inappropriately sharing your user ID or password to allow an individual to obtain information to which they normally would not have access.
- Deliberately damaging or disrupting a computer system (hardware or software) or intentionally attempting to "crash" network systems or programs.
- Attempting to gain unauthorized access to internal or external computer systems.
- Attempting to decrypt system or user passwords.
- Unauthorized copying of system files or software programs.

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 the 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 Technology Services Manager. If permission to connect these tools/peripherals is granted, the employee must follow provided directions and procedures for protecting the City's computer network.
- Personal files should not be stored on City computer equipment. This included 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. The Technology Services Manager will delete these types of files if found on the network, computers, or other City-owned equipment. Exceptions are recordings that the City has created or purchased.
- 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 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 their job duties. Requests for new or different equipment should be made to your supervisor/Department Head, who will forward the request to Technology Services Manager.

The City will not supply laptop computers based solely on the desire of employees to work offsite. 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 strictly 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.

Telephones

The City Administrator may determine that some employees carry or use cellular telephones because of the nature of the work. Employees are responsible for all calls made or retrieved while the cellular phone is assigned or they are in possession of a cellular telephone. Employees may use cellular telephones for personal calls on an occasional basis for important calls. Employees may not use City telephones to conduct commercial business or any activity which may cause the perception of misuse. Employees are responsible for any charges resulting from unauthorized or personal use of cellular telephones.

Employees may have personal cellular telephones; however, they may only be used for emergencies or during break or lunch periods. Employees may not use personal telephones to conduct commercial business during their work day.

Any violation of this policy may result in loss of telephone use by the employee, along with other disciplinary procedures.

Checking out Equipment

When employees check out portable equipment, such as laptop computers, they are expected to provide appropriate "common sense" protection against theft, breakage, environmental damage, and other risks. An employee who fails to exercise "common sense" protection may be subject to discipline, including the cost of replacement or repair. Desktop computers and attached devices are not to be removed from City buildings without authorization.

Software

In general, the City will provide the software required for an employee to perform their job duties. Requests for new or different software should be made to your supervisor/Department Head, who will forward the request to the Technology Services Manager.

Employees shall not download or install any software on their computer without the prior approval from the Technology Services Manager. Exceptions to this include updates to software approved by Information Technology such as Microsoft updates, or other productivity software updates. The Technology Services Manager 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 City authorized staff and without notice to the employee.

Employees must adhere to these email requirements:

- Never transmit an email that you would not want your supervisor, other employees, city officials, or the media to read or publish (e.g., avoid gossip, personal information, swearing, etc.).

- Use caution or avoid corresponding by email regarding confidential matters (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 at the basic level. Employees may elect to share all details of their calendar at their discretion. Supervisors/Department Heads should determine if others may schedule meetings on their behalf in the their calendars.

Instant Messaging

Due to data retention concerns, Instant Messaging (IM) is only allowed for transitory discussions and should be deleted after use. The City only allows IM via Microsoft Teams. 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 other IM software package on their City computer.

Personal Devices

Employees should not 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 scenario, and agree to grant access to or temporarily surrender their personal devices should such a situation arise.

Security

Passwords

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

- Passwords must be at least twenty 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 are based on the FBI CJIS policy and may be changed as necessary, as determined by the Technology Services Manager.
- Passwords must be provided to the Technology Services Manager when requested. Failure to provide the password may result in employee disciplinary action.
- Passwords should not be shared with 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; the

Technology Services Manager will not provide access to staff accounts without approval of the 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 365 days when prompted, or on another schedule as determined by the Technology Services Manager.
- Remembering passwords is the responsibility of the employee. Technology Services staff will not keep a plain-text record of employee's passwords.

Network access

Non-City-owned computer equipment used in the City's building should only use the public wireless connection to the Internet. Under no circumstances should any non-City-owned equipment be connected to the City's private computer network. Exceptions may be granted by the Technology Services Manager.

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:

- Remote access to the City's network requires a request from a supervisor and approval from the Technology Services Manager. Remote access privileges may be revoked at any time by an employee's supervisor/Department Head.
- 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 may 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 open wireless access points, regardless of the technology used to connect.

Internet

The following considerations apply to all uses of the Internet:

- 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, do not visit it.

- If an employee's use of the Internet is compromising the integrity of the City's network, Technology Services staff may temporarily restrict that employee's access to the Internet. If Technology Services staff does restrict access, they will notify the employee, HR, and the employee's supervisor/Department Head 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/Department Head in consultation with the Technology Services Manager.

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/Department Head. If you are unsure how to create an appropriate file structure for saving and storing electronic information, contact the Technology Services Manager.

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

- All electronic files must be stored on identified network drives and folder locations. 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 the 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 in designated locations 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 by Technology Services 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.
- 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 approved by the Technology Services Manager.