City of Ivanhoe, Minnesota
Computer Use Policy (3.2025)

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 the 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 the City Council or designee.

Beyond this policy, the city's administrator or IT Support 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 city administrator. 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. IT Support 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 to be inconsistent with City activities. If there is any question about whether a use is appropriate, it should be forwarded to the city administrator or IT Support 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 council.

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.

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 the city council.

Employees shall not download or install any software on their computer without the prior approval of the city administrator. Exceptions to this include updates to software approved by Information Technology such as Microsoft updates, or other productivity software updates. City administrator, IT Support 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. All employees given a city email address shall use the email address assigned for all city communication.

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.

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 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.

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.

Personal computer equipment may not be connected to the City's network without prior approval of the 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), or Windows Remote Sessions. 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 city administrator. Remote access privileges may be revoked at any time by an employee's supervisor.
- 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.
- 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, city administrator, IT Support staff may temporarily restrict that employee's access to the Internet. If IT Support staff does restrict access, they will notify the employee, and the employee's supervisor 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.
- Employees may use low-risk data with Artificial Intelligence (AI) technology to perform their work. Low-risk data is defined by Minnesota Statutes Chapter 13 as "public" and is intended to be available to the public. If you are unsure whether the data you enter into AI applications is classified as public data, consult your City's responsible authority or designee prior to using AI technologies. All data created with the use of AI is to be retained according to the City's records retention schedule.

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 administrator.

Employees must adhere to these guidelines 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 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 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; IT Support can assist in the encryption of media.

Policy Change. This policy replaces all previous policies covering the same or similar topics. This policy may be reviewed and changed at any time.

Adopted by the City Council of the City of Ivanhoe this 11th day of March, 2025.

Signed: Attest:

_____ _____

Mayor, Shad Lipinski Dianne Beckendorf, City Administrator

Employee signature

I have received and read the Computer Use 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 and or termination.

_____ (Print Employee Name)

_____ (Employee Signature)

_____ (Print Department Name)

_____ (Date)