Policy 119 Department Computer Usage

Effective Date: November 13th, 2007 **Revised Date: April 30th, 2024**

Section 1 **Purpose**

The City of Wayzata's maintenance of information technology (IT) systems is key to meeting the City's operational, financial and other needs. City IT systems and services are provided for the efficient exchange of information and to assist staff in completion of their duties. However, the availability of such technology increases the risks associated with sharing of information and resources. The purpose of this policy is to protect and maintain the City's IT systems in a secure environment and to eliminate uses of the City's IT resources that might place the City, its residents and/or its IT system users at risk.

Section 2 **Coverage under this policy**

Employees, as well as contractors, vendors and others who have access to the City's IT systems and services are required to abide by this policy. The City Manager and Department supervisors shall ensure that contract documents a) require contractors and vendors to comply with City security policies, guidelines and procedures; and b) protect the City's ownership and copyrightable interests in all programs and software developed on behalf of the City.

Section 3 **Access to City IT systems and services: passwords and security**

Only those individuals with an authorized user identification and password shall be allowed access to City IT systems and services. Issuance of a user identification and password requires the approval of a department head or the City Manager. Each user is responsible for all activity that occurs in connection with the use of his or her assigned user identification, and for the protecting information which they create, receive or to which they have access. It is therefore crucial that users not reveal their passwords to anyone other than the City's system administrator, nor should the user allow anyone else to use any computer password or user identification, or attempt to log on or use another's user's email or other accounts. Users whose relationship with the City terminates will have their IT system privileges revoked immediately.

Section 4 **Personal use of City IT systems**

Access to the City's IT systems and services is provided to users for the benefit of the City and its residents, and use of City-owned or leased IT systems and services are generally intended only for official business purposes. Incidental or occasional personal use of IT systems and services may be permitted subject to the limitations of this policy, provided such,

A. Does not interfere with that individual's or any other individual's duties or routine business activities;

B. Does not result in additional expense to the City or result in the consumption of City resources;
C. Does not require modification to software or other system components;
D. Is not for political, religious, unlawful or illegal practices, personal financial profit or other promotional activities;
E. Does not contain or imply threatening, obscene, or abusive language, contain or imply harassing, demeaning or sexually explicit statements or materials, or otherwise violate the Police Department's Workplace Conduct Policy.

119.4.1 Any messages or information sent by a user to another individual, whether inside or outside the City's network, including emails, bulletin board postings, Web logs etc., are statements that reflect on the City. All communications sent by users via the City's email system or over the Internet must comply with this and other City policies.

Section 5 Communications are not private

Use of the City's IT systems and services involves the creation of documents and other materials which are and will remain sole property of the City. These documents, including email messages sent and received by employees or others via City IT systems, are NOT private. In addition, even though an electronic message may be deleted from the email system, a record of it remains on the computer system, either on regular backups or in other ways. Email messages and Internet files, like correspondence and other documents, may be read by other users or by those outside of the City under certain circumstances, including but not limited to the following:

A. During regular maintenance of computer systems;
B. When the City has a business need to access a user's computer;
C. When the City receives a legal request, from law enforcement officials or in ongoing legal proceedings, to disclose electronic communications; or
D. When the City has reason to believe that any user is using any IT system or service in violation of this or other City policy, including the Police Department's Workplace Conduct Policy.

Section 6 Data Privacy

Users who work with private and/or confidential data, whether designated as such under the Minnesota Governmental Data Practices Act, other law, City policy or other form of designation, must maintain the confidential or private nature of such data by protecting it from inappropriate disclosure via the City's IT systems and otherwise. Private, confidential or other sensitive data should be reasonably protected during electronic transfer at all times.

Section 7 **User signatures on electronic communications**

All messages communicated on the City's email system must contain the User's name and position with the City. Each user is responsible for the content of all text, audio or images that he or she places or sends using the City's IT systems. No email or other electronic communications may be sent which hide the identity of the sender or represent the sender as someone else or someone from another organization.

Section 8 **Harassment or other offensive conduct**

All communications conducted through the City's computer system must be professional and businesslike. It is a violation of City policy to create, transmit, receive or send any electronic communications which are obscene, hostile, degrading or otherwise offensive in nature, including but not limited to any offensive references to any person based on that person's sex, sexual orientation, race, nationality, political affiliation, disability, religion or membership in any organization. The police department's Workplace Conduct Policy against sexual and other forms of harassment apply fully to the City's IT systems and services.

Section 9 **Software installation and viruses**

To prevent computer viruses from being transmitted to or through the City's IT systems, unauthorized downloading of any software is strictly prohibited, including any such materials received as e-mail attachments or from online service. Only authorized City personnel are permitted to install hardware and software or to make changes to the configuration of operating systems on City owned or leased equipment. Installation and/or use of personally owned software and hardware components on City owned or leased equipment is prohibited without department head or City Manager approval.

Section 10 **No unofficial data files**

Users are prohibited from maintaining unofficial data files or computer programs (i.e. files or programs not related to City business) on City owned or leased IT systems.

Section 11 **Copyright issues**

Employees and contractors may not reproduce, distribute or otherwise transmit any copyrighted materials belonging to any third party, and may only transmit such materials belonging to the City with proper authorization and for proper business purposes. Any reproduction, distribution or other transmission of third party copyrighted material must be authorized by your supervisor or the City Manager and can be done only after receiving the appropriate license or other consent from an authorized representative of the copyright owner.

Section 12 City data on personally owned systems

Subject to applicable legal privileges and confidentiality requirements, all City data entered on personally owned computers remains the property of the City and is subjected to disclosure upon the demand of authorized City personnel at any me time.

Section 13 Maintenance

Employees and contractors are encouraged to conduct frequent purges of electronic messages or computer files that no longer pertain to current action items. Whenever practicable, e-mail messages should be deleted after opening and reading, and items located in deleted items files and/or electronic trash bins should also be deleted on a regular basis.

Section 14 Unlawful or malicious conduct

City resources shall not be used for any unlawful purpose or practice. Malicious conduct of any kind using the City's IT systems is also strictly prohibited. Such conduct includes, but is not limited to, the creation or transfer of any virus or other malicious code, as well as acts of vandalism or other malicious attempts to destroy or damage data and/or to disrupt or degrade the City's computer system in any manner.

Section 15 Mobile Data Computing (MDC)

All aspects of the City's Computer Usage policy apply to the use of MDC's that are installed in all police department vehicles. Employees of the police department must also be aware that all MDC transmissions are discoverable as public data.

Section 16 Investigative Purposes

At certain times, members of the Wayzata Police Department will become involved in the investigation of such crimes as, but not limited to child pornography, prostitution or employment background checks. During the course of the investigation, officers shall be allowed to access web sites that would normally be in violation of this policy. Access to these web sites shall strictly be used for
investigative purposes only. The Chief of Police should also be notified in advance of the potential accessing of forbidden sites.

Section 17 Policy Enforcement

All activity on City IT systems and services is subjected to monitoring by authorized individuals to ensure system integrity and compliance with this policy and other City policies and standards. Such monitoring may include access to systems without notice to the user. Any employee who violates this policy or uses e-mail or any other electronic system for improper purposes will be subjected to revocation of IT system privileges, as well as other discipline up to and including discharge. Misuse of City property, including programs and data files, may also be subject to criminal sanctions.

Section 18 Reporting of violations; no reprisal

Employees are encouraged to report sensitive security issues and violations directly to their supervisor or the City Manager. Employees who so report will not be subject to reprisal by the City or its authorized representatives.