COMPUTER, EMAIL & INTERNET USE
POLICY NO: 207-P

- Applies To: All Departments
- Effective Date: 11/01/2026
- Associated References: City Freedom of Information Act (FOIA) Policy, 244P Artificial Intelligence Personnel Policy

Purpose:

This policy establishes guidelines for the proper, secure, and ethical use of the City of Traverse City's computers, mobile devices, network resources, internet access, electronic mail (e-mail), software, and cloud applications. All employees and authorized users must use these resources in a professional, ethical, and lawful manner, and are responsible for adhering to their respective department policies regarding their use.

The information created, stored, sent, or received through the use of these systems is the property of the City of Traverse City, not the individuals who create or access them. Federal and state laws (including the Michigan Freedom of Information Act) may require the disclosure or reproduction of this information to third parties.

Definitions:

A. **Computer Network:** Any combination of computers, servers, mobile devices, network equipment, cloud environments, printers, audio/visual devices, or telecommunication systems interconnected to transmit or receive data.
B. **Electronic Mail (E-mail):** Exchange of digital messages, documents, and calendar invites. An e-mail includes the message content, transaction metadata (timestamps, delivery records, headers, recipient lists), and any attached files.
C. **Public Record:** A writing prepared, owned, used, in the possession of, or retained by a public body in the performance of an official function, from the time it is created. Public record does not include computer software.
D. **Records Management:** The policies, procedures, and applicable retention and disposal schedules governing the creation, maintenance, preservation, storage, and lawful disposition of City records, including State of Michigan-approved general and agency-specific schedules.

E. **Confidential Information:** Authorized users shall safeguard confidential, privileged, sensitive, and legally protected information obtained through City employment. Such information will only be accessed, used, transmitted, or disclosed as authorized and necessary for official duties. Employees shall use City-approved security measures when transmitting sensitive information and shall not forward such information to personal accounts or unauthorized recipients.

Scope:

GENERAL COMPUTER & TECHNOLOGY POLICIES

1. **Authorized Access:** Only current City employees, official volunteers, or explicitly authorized contractors may access City technology resources.
2. **Acceptable Use:** Authorized users shall use the City's internet access primarily for authorized work-related purposes.
3. **Prohibited Use:** City computer resources and internet connections shall not be used for illegal activity, gambling, accessing or distributing pornographic or offensive material, harassment, or unauthorized personal commercial gain.
4. **Software & Copyright:** Unlawful copying, installing, or downloading of copyrighted software, unauthorized applications, or unlicensed media is strictly prohibited.
5. **Generative AI & Third-Party Cloud Tools:** Employees shall not enter confidential, sensitive, proprietary, or personally identifiable information (PII) into non-approved, third-party Artificial Intelligence (AI) tools or unapproved web applications (see 244P Artificial Intelligence Policy).
6. **Electronic Messaging:** Work-related communications conducted through text messages, instant messaging applications, collaboration platforms, or similar technologies are subject to the same conduct, confidentiality, records-retention, and preservation requirements applicable to City email. Employees shall use City-approved communication platforms for official business and preserve public records in accordance with applicable retention schedules.

INTERNET AND NETWORK USE

Access to the Internet is provided as a business tool and professional benefit. Internet access is primarily for conducting City business, research, and official communication consistent with City goals and objectives.

Acceptable Work-Related Uses:

- Research & Education: Communication with professional associations, peer governments, universities, and industry experts to facilitate City business. Registering and attending training courses and conferences. Researching standards, specifications, existing conditions, environmental data, potential and existing vendors, materials, or other city and project related items.

- Public Communication: Distribution of information to the general public in accordance with City communication guidelines and FOIA rules.
- Professional Collaboration: Incidental communication among professionals discussing work-related fields.

Incidental Personal Use:
Employees may engage in minor, incidental personal internet or network use outside of work hours (or during designated breaks), provided it does not interfere with job duties, compromise security, or violate City policies.

Monitoring and Privacy:

Employees should have no expectation of personal privacy when using City-owned equipment, accounts, networks, or communication systems, except as otherwise protected by law. The City reserves the right to access, inspect, monitor, retrieve, and review information contained in or transmitted through City systems for legitimate business, security, records-management, or investigative purposes, consistent with applicable law. Monitoring shall be performed by authorized personnel.

E-MAIL & DIGITAL COMMUNICATIONS

City Electronic Communications: Electronic messages created, received, transmitted, or stored through City-provided accounts or systems are subject to City management, access, monitoring, and retention requirements, consistent with applicable law. Communications concerning official City business may constitute public records regardless of the device, account, or platform used.

Anonymity & Impersonation: Employees may not send anonymous e-mails or misrepresent their identity, except during authorized law enforcement or official city investigations.

Official Representation: Statements made via official City e-mail or communication platforms are attributable to the City of Traverse City. Employees must not disclose confidential or non-public data unless authorized in the performance of official duties.

Personal Devices and Accounts: Employees shall conduct City business through City-approved communication systems and accounts unless otherwise authorized. Employees shall not use personal email accounts, messaging applications, or cloud storage services to conduct or store official City business without authorization. Any City business conducted through a personal device or account remains subject to applicable records-retention, preservation, and disclosure requirements. Employees must promptly transfer or preserve such communications through an approved City system as directed.

Remote Access and Devices: Employees shall access City systems remotely only through approved devices, applications, and secure connections. Unauthorized devices, removable storage media, software, or external systems shall not be connected to City networks without IT approval.

E-MAIL/MESSAGE RETENTION AND DISPOSAL

Public Record: Official correspondence, policies, contract revisions, purchase approvals, citizen complaints, and personnel documentation.

- *Retention:* Retain according to the official Records Management Handbook schedule.

Work-related Appointments, Tasks, & Notes: Daily performance logs, calendars, training approvals, and task tracking.

- *Retention:* Retain in accordance with the applicable approved records retention schedule based on the nature and purpose of the record.

Transitory Record: Short-lived communications with minimal administrative value (e.g., meeting reminders, requests for minor documents, acknowledgments).

- *Retention:* Dispose of when authorized by the applicable approved retention schedule.

Non Record Materials: Personal communications unrelated to City business, unsolicited advertisements, and other materials that do not document official City functions or activities.

- *Retention:* Delete when no longer needed, subject to applicable preservation requirements.

Employee Responsibilities:

Employees are responsible for appropriately maintaining and preserving work-related electronic communications, including relevant attachments, in accordance with City procedures and applicable retention requirements.

Litigation & FOIA Holds: No e-mail or record may be destroyed if it is subject to an active FOIA request, administrative audit, or ongoing litigation, regardless of normal retention expiration.

Recordkeeping Responsibility: Employees responsible for a particular City function, project, transaction, or matter shall ensure that related electronic records are retained in the appropriate City recordkeeping system. Employees shall not assume that another sender or recipient has retained an official record unless responsibility for maintaining the record has been clearly established. Duplicate copies may be deleted when authorized by the applicable retention schedule and when the official record has been appropriately preserved.

Thread Retention: Employees may retain a complete, consolidated email thread in lieu of duplicative individual messages, provided the retained thread accurately preserves all relevant communications, attachments, dates, participants, and substantive information. Individual messages containing unique information, attachments, or decisions must be separately preserved when necessary to maintain a complete official record.

Archiving & Organization: Employees must organize e-mail records systematically within approved City cloud/network storage environments. Assistance with setting up automated archival policies can be obtained through the IT Department. All employees shall follow applicable department policies for saving to the shared drive and are expected to familiarize themselves with the appropriate locations and adhere to the process.

Storage Location & Data Backup: Employees must save all official work documents and files to the designated department City Shared Drive. Employees shall not save documents to local computer desktop drives, as local desktop drives are not backed up and files stored there are subject to permanent loss.

Departing Employees: Department Heads, in coordination with the Technology Department, shall ensure that the digital records and e-mail accounts of departing employees are properly organized, preserved, and archived in the designated shared drive in accordance with City records retention requirements.

IT & CYBERSECURITY

Access Controls & Passwords: Access credentials including but not limited to usernames, passwords, pins, etc., are the property of the City. Authorized users must maintain unique passwords, utilize Multi-Factor Authentication (MFA) where required, and never share credentials.

System Security: Authorized users must not attempt to bypass security filters, disable antivirus/endpoint protection software, or grant unauthorized network access to third parties. Hardware Information: Unauthorized disclosure of internal system architectures, network settings, or security configurations to outside parties is strictly prohibited.

Cybersecurity Awareness: Employees shall complete required cybersecurity training and exercise reasonable care when opening attachments, accessing websites, responding to suspicious communications, or handling City information.

Incident Reporting: Suspected security breaches, phishing attempts, accidental disclosures, lost devices, or unauthorized access shall be reported immediately to the IT Department, regardless of whether actual harm is known.

FOIA AND LITIGATION COORDINATION

In compliance with the Freedom of Information Act, the City maintains a designated FOIA coordinator. The CIty's FOIA Coordinator is the City Clerk.

FOIA Compliance: Upon request from the City Clerk or designated FOIA Coordinator, employees must promptly search and provide all relevant e-mail and digital records.

Records Preservation and Legal Holds: Employees shall not delete, alter, destroy, or otherwise dispose of records that are subject to a pending FOIA request, audit, investigation, litigation, reasonably anticipated litigation, or a preservation directive issued by the City. Employees shall immediately notify the City Clerk, City Attorney, or designated official upon receiving notice of a matter requiring preservation. Applicable records shall remain preserved until the City authorizes release of the hold, notwithstanding otherwise applicable retention or deletion schedules.

IT Notification: The FOIA Coordinator may notify the IT Department to suspend automated deletion policies on affected accounts until legal matters or FOIA requests are fully resolved.

ENFORCEMENT AND VIOLATIONS

Nothing in this policy is intended to restrict employees from engaging in legally protected activities, including protected concerted activity, lawful whistleblower disclosures, communications with governmental agencies, or exercising constitutional or statutory rights. Employees remain responsible for protecting confidential information as required by law.

Violation of this policy may lead to disciplinary action up to and including termination of employment, revocation of network access privileges, and potential civil or criminal liability where applicable laws are broken.

Questions regarding the interpretation of this policy should be directed to your Department Head or Human Resources.

Approved By: Benjamin Marentette on 10/28/2026 Signature:	HISTORY: Supersedes Executive Order No. 315(June 20, 2008) Supersedes Personnel Policy 207P July 2011