

INFORMATION TECHNOLOGY

Revised September 2026

SECTION: 12

A. PURPOSE

1. This Section establishes expectations for the appropriate and responsible use of the City's Computer Systems and Information Technology. Employees are expected to use City Computer Systems and Information Technology resources in a manner that protects City data, supports City operations, promotes system security, and complies with applicable laws and regulations.
2. Technology and cybersecurity threats are constantly changing, so this Section cannot address every situation or type of technology that may arise. The City may establish, change, or temporarily suspend IT practices, procedures, restrictions, or requirements as needed to address operation needs, new technology, security threats, system vulnerabilities, or other risks to City systems and data.

B. DEFINITIONS

As used in this Section, the following have the stated meanings:

1. Access to or accessing – Viewing, opening, or searching for, or otherwise interacting with electronic information or material whose content the employee knew or reasonably should have known the content of.
2. Bring Your Own Device (BYOD)/Personal Device – An employee-owned electronic device, used to access City systems or conduct City business including laptop, tablet, mobile phone, and similar device.
3. City Business – Activities, communications, transactions, or other matters conducted on behalf of or relating to the official business, operations, functions, or responsibilities of the City.
4. Computer Systems and Information Technology – Technology resources owned, leased, licensed, hosted, managed, or otherwise authorized by the City for City operations, including hardware, software, computers, mobile devices, networks, servers, storage devices, e-mail, Internet access, electronic records and communications, and cloud-based, hosted, remote, or third-party applications, platforms, and services used for City business.
5. Electronic Records – Records in electronic or digital form that are created, received, maintained, or used in connection with City business, regardless of where the records are stored or the device or system on which they are created or maintained. This may include e-mail, text messages, electronic files, photographs, social media content, and other electronic communications or data. Electronic records related to City business may be subject to City records management and retention requirements, including when they are created or maintained on an employee's personal device.

INFORMATION TECHNOLOGY

Revised September 2026

SECTION: 12

6. Government Records Access and Management Act (GRAMA) - Utah's law governing the management, classification, retention, and access to government records. GRAMA establishes what constitutes a government record and provides requirements and procedures for access to those records.
7. IT or IT Department – City staff members assigned to Information Technology (IT) Department or employees provided with duties in support of the City's IT Department.
8. Social Media – Online platforms, applications, and services used to create, share, publish, or exchange information or content, including social networking sites, blogs, websites, forums, discussion boards, chat platforms, and similar services.

C. PRIVACY & MONITORING

The City's Computer Systems are provided for City business. Employees have no expectation of privacy when using City Computer Systems. The City may, at its discretion and as permitted or required by law, monitor, review, access, copy, or disclose information, data, files, and communications stored on or transmitted through City computer systems, whether related to City business or personal in nature, with or without notice or the employee's consent. The City may take these actions as necessary to conduct City business, protect City systems and data, investigate suspected misconduct or security concerns, comply with legal or records requirements, or serve other legitimate City purposes.

D. HARDWARE, SOFTWARE, CLOUD-BASED SYSTEMS, AI, AND LICENSES

1. **Hardware.** The City purchases and owns hardware used for City business, which is administered by the IT Department or its designee. Employees may not use or install hardware without approval from the IT Department. Requests for new hardware must be submitted through the IT Department for evaluation of compatibility, cost, security, and other considerations. Hardware purchases must comply with the City's purchasing policies and procedures, and applicable IT Department requirements. The IT Department maintains an inventory of City hardware with a value of \$500 or more. City hardware may be used, transferred, relocated, or removed only as authorized by the City or IT Department.
2. **Software and Licenses.** The City purchases and licenses software for use on City Computer Systems. Employees may not copy, transfer, share, loan, or otherwise use City software, licenses, or related documentation. Software may not be installed on City Computer Systems without appropriate approval from the IT Department. Requests for new software must be submitted through the IT Department for evaluation of compatibility, cost, security, licensing, and other considerations. Software purchases and licenses must comply with the City's purchasing policies and procedures and applicable IT Department requirements.

INFORMATION TECHNOLOGY

Revised September 2026

SECTION: 12

3. **Cloud-based Systems.** Employees may use cloud-based services, storage platforms, and software services that have been reviewed and authorized by the IT Department. Approved cloud services are managed in accordance with City compatibility, security, operational, data management, records retention, and privacy requirements. Employees may not store, transmit, upload, or share confidential, sensitive, protected, or non-public City information through unauthorized cloud-based systems or personal accounts. The City may restrict, suspend, audit, or discontinue access to any cloud-based application or service as necessary to protect City systems and information or to meet legal requirements.
4. **Artificial Intelligence (AI).** Employees may use only artificial intelligence (AI) tools, applications, and services that have been reviewed and authorized by the IT Department. AI tools must be used in a manner that protects City information and complies with City policies, applicable law, records retention requirements, and cybersecurity standards. Employees may not enter confidential, sensitive, protected, or non-public City information into an unauthorized AI tool or use AI in a manner that creates a security, privacy, legal, or other risk to the City. The IT Department may maintain and update a list of approved AI tools and may restrict, suspend, or prohibit the use of any AI tools as necessary to protect the City systems and information. Employees remain responsible for reviewing and verifying AI-generated content before using or relying on it for City business.

E. PASSWORDS, AUTHENTICATION, AND COMPUTER SYSTEMS SECURITY

1. **Protecting Credentials.** Passwords, passcodes, multi-factor authentication (MFA), and other authentication credentials protect the City's Computer Systems and information. Employees are responsible for keeping their City credentials secure and confidential and for taking reasonable steps to prevent unauthorized access to their accounts, devices, and City information.
2. **Security Requirements.** The IT Department may establish, implement, modify, and enforce password, authentication, and other security requirements necessary to protect City technology resources and information. These requirements may include password standards, password expiration, MFA, password management tools, device security, account access restrictions, and procedures for responding to compromised credentials or security incidents. Employees shall comply with all security requirements established by the IT Department. The IT Department may immediately implement or modify security requirements as necessary to address cybersecurity threats, changes in technology, or other security concerns.
3. **Sharing Credentials.** Employees shall not share passwords, passcodes, MFA codes, authentication credentials, or other account access information with another person, including coworkers, vendors, contractors, or other third parties, except

INFORMATION TECHNOLOGY

Revised September 2026

SECTION: 12

through a procedure specifically authorized by the IT Department. Employees shall not approve or respond to an MFA request that they did not initiate.

4. **Cybersecurity Threats.** Employees are expected to use reasonable caution when responding to e-mail, messages, links, attachments, MFA requests, and other communications that may present a cybersecurity risk. Employees shall immediately notify the IT Department if they suspect that a password, account, device, or other City information or technology resource has been compromised.

F. LOST OR STOLEN DEVICE REQUIREMENTS

1. **Reporting Requirements.** Employees shall immediately report the loss, theft, or suspected loss or theft of any City-owned device or any personal device used to access City Computer Systems or conduct City business to the IT Department and their supervisor. Employees shall report the incident as soon as reasonably possible and should not wait until the next workday.
2. **Security Measures.** Employees shall cooperate with the IT Department in taking reasonable steps to protect City systems and information following the loss or theft of a device. The IT Department may remotely lock, disable, locate, or erase a device; reset passwords or authentication credentials; suspend or terminate access; or take other security measures necessary to protect City systems and information.
3. **Personal Devices.** When a personal device is used for City business, employees are responsible for promptly reporting its loss or theft when City systems, accounts, or information may be accessed through the device. The City will take reasonable steps to limit security measures or requests for information to City business and City information.
4. **Employee Responsibility.** Employees shall not attempt to bypass, disable, or interfere with security measures implemented by the City in response to a lost or stolen device and shall follow any instructions provided by the IT Department to secure City systems and information.

G. PERSONAL USE OF CITY COMPUTER SYSTEMS – PERMITTED & PROHIBITED

Tooele City's Computer Systems are provided primarily for City business and generally may not be used for personal purposes. The City recognizes that limited, incidental personal use may occasionally occur during the workday and permits such use when it does not interfere with work responsibilities, violate City policy, or create a risk to City systems or information. Employees should not expect privacy when using City Computer Systems, including when engaging in permitted incidental personal use. Such use may be monitored, reviewed, accessed, copied, or disclosed by the City as provided in this Section and as permitted or required by law. Incidental personal use is not permitted for any of the following:

INFORMATION TECHNOLOGY

Revised September 2026

SECTION: 12

1. Unlawful activity
2. Gambling
3. Offensive/discriminatory/pornographic/sexually explicit material
4. Political or religious advocacy unrelated to City business
5. Personal commercial/business activity
6. Unauthorized software/downloads
7. Anything that creates a security risk
8. Excessive personal use or activities that interfere with work
9. Use by family or non-City employees
10. Any other use that may compromise the integrity of the City Computer Systems
11. Any use violating law or City policy

H. E-MAIL GUIDELINES & EXPECTATIONS

1. **Business Use and Security.** Employees shall use electronic mail (e-mail) professionally and with the same level of care expected of other City business communication. E-mail messages may constitute government records and may be subject to retention, disclosure, or other requirements under applicable law. Employees should use caution when sending information through e-mail because messages may be forwarded, copied, intercepted, or viewed by unintended recipients, particularly when sent outside the City's network. Passwords, MFA codes, or other authentication information shall not be transmitted through e-mail.
2. **Phishing and Malicious Content.** Employees shall use caution when opening e-mail, attachments, links, or other electronic content. Suspicious messages may contain phishing attempts, malicious software, fraudulent requests, or other threats to City systems and information. Employees should not open suspicious attachments, click unknown or unexpected links, or provide credentials or other sensitive information in response to an unsolicited message. Suspected phishing or other suspicious e-mail should be reported to the IT Department.
3. **E-mail Signatures.** Employees shall use the e-mail signature format established by the City.

I. USE OF PERSONAL DEVICES (BYOD)

1. **Authorization.** Employees may use personal electronic devices to conduct City business only when authorized by their department and in accordance with requirements established by the IT Department. Department approval alone does not authorize a personal device to connect to City Computer Systems or access City accounts, applications, or information. The IT Department may establish minimum security, compatibility, and configuration requirements for personal devices used for City business.

INFORMATION TECHNOLOGY

Revised September 2026

SECTION: 12

2. **Security Requirements.** Employees who use a personal device for City business are responsible for maintaining the device in accordance with applicable IT security and BYOD requirements. Employees shall take reasonable steps to protect City information accessed or stored on the device and shall promptly report the loss or theft of a personal device when City systems, accounts, or information may be accessed through the device.
3. **IT Support.** Employees are responsible for the operation, maintenance, security, and functionality of their personal devices. The IT Department may provide limited assistance when necessary to enable an employee to perform City business, but such assistance is provided at the employee's request and within the IT Department's capabilities. The IT Department is not responsible for maintaining, repairing, configuring, or supporting a personal device for non-City purposes.
4. **Risk of Data Loss.** IT assistance with a personal device may require changes to the device, including security settings, applications, configurations, or access controls, and may result in the loss or alteration of personal data. Employees are responsible for backing up and protecting personal information stored on their devices before requesting or allowing IT assistance. The City is not responsible for loss of personal data resulting from IT assistance or actions taken to protect City systems or information.
5. **City Records and Legal Obligations.** Employees should understand that information related to City business stored or communicated on a personal device may be subject to applicable records retention, public records, litigation, audit, investigation, or other legal requirements. When necessary to comply with those requirements, the City may require employees to provide access to or copies of City-related information maintained on a personal device and, in appropriate circumstances, may require the device to be made available for examination or other lawful purposes. The City will make reasonable efforts to limit such requests to information related to City business. The City is not responsible for providing a replacement device when a personal device must be made available for these purposes.
6. **Separation of Personal and City Information.** Employees using personal devices for City business are responsible for keeping City information appropriately secured and, when reasonably possible, separated from personal information. Employees shall not use personal accounts or unauthorized applications or storage services to store or transmit City information.
7. **Records Retention.** City records created, received, or maintained on a personal device while conducting City business remain subject to applicable records retention and public records requirements, including the Government Records

INFORMATION TECHNOLOGY

Revised September 2026

SECTION: 12

Access and Management Act (GRAMA). Employees are responsible for complying with City records retention requirements when using a personal device for City business. See Section N, Electronic Records and Records Retention, for additional requirements.

J. CITY WEBSITES

1. City websites and official webpages are provided to communicate with the public, provide access to government information and services, and promote authorized City programs, events, and activities. The Mayor has final authority over official City websites, including their content, appearance, and use. Only employees designated by the City as website administrators or authorized content managers may create, modify, or post content to City websites.
2. Content posted or maintained on City websites must comply with applicable law and City policies and support legitimate City purposes. City websites may not be used for unauthorized classified ads, political advocacy, or endorsements or opposition related to social issues, causes, or religions. Commercial advertising is permitted only when it relates to a legitimate public interest, City-sponsored program, community partnership, economic development effort, or other authorized City activity.

K. CITY USE OF SOCIAL MEDIA

1. Official City social media accounts may be used to communicate with the public, promote City programs and services, provide public information, and share time-sensitive or emergency information. The Mayor may establish and enforce policies, procedures, and standards governing the creation, management, security, retention, and use of official City social media accounts.
2. Only employees authorized by the City may create, manage, access, or post content on behalf of the City through official social media accounts. Employees shall use social media professionally, for authorized governmental purposes, and in compliance with applicable law and City policies.
3. The City may monitor, restrict, remove, retain, or archive content or user interactions as permitted or required by law or City policy, including to address security concerns, public records requirements, violations of City policy, or content that is inconsistent with the purpose of the account. City social media accounts, including their usernames, passwords, administrative access, content, and related data, remain under the control of the City.

INFORMATION TECHNOLOGY

Revised September 2026

SECTION: 12

L. EXCEPTION FOR LAW ENFORCEMENT AND LEGAL PURPOSES

Law enforcement personnel and legal personnel may engage in otherwise restricted social media activity when reasonably necessary for an authorized law enforcement, investigative, intelligence-gathering, prosecutorial, litigation, compliance, or legal purpose. Such activity requires advance supervisory approval.

M. EMPLOYEE PERSONAL USE OF SOCIAL MEDIA

1. Employees may use social media for personal purposes and are generally responsible for their personal social media activity. Personal use of social media does not, by itself, constitute City business or an official statement of the City. Employees may not, however, use personal social media to disclose confidential, protected, or non-public City information, represent that they are speaking on behalf of the City without authorization, or otherwise violate an applicable City policy or law.
2. Employees should exercise care when personal social media content identifies them as a City employee or includes a City uniform, badge, logo, vehicle, facility, equipment, or other City property. Such use shall not imply that the City endorses, sponsors, or supports the employee's personal views, activities, products, services, organizations, or causes. Employees may not use their City position, uniform, or City property for personal or political purposes when prohibited by law or City policy.
3. Employees are expected to comply with applicable City policies concerning confidentiality, workplace conduct, harassment, discrimination, and professionalism when their social media activity implicates those policies. Nothing in this Section is intended to prohibit lawful personal expression or to require employees to refrain from identifying themselves as City employees on personal social media.

N. STORAGE AND RETENTION OF ELECTRONIC RECORDS

1. **Records Retention.** Electronic records are subject to the same records retention requirements as records in other formats. Employees shall retain and dispose of electronic records in accordance with the City's applicable records retention schedules and policies. Employees should consult their department's retention requirements or the City's Records Officer when they are unsure how long a record must be retained.
2. **City Records on Personal Devices.** City records created, received, or maintained on a personal device or account while conducting City business remain subject to applicable records retention and public records requirements, including the Government Records Access and Management Act (GRAMA). Employees may

INFORMATION TECHNOLOGY

Revised September 2026

SECTION: 12

not delete, alter, or destroy a City record outside of the applicable retention requirements.

3. **Cloud Storage and Services.** Employees may use only cloud-based storage services and applications that have been approved by the IT Department for City business. Employees shall not store City information, particularly confidential, sensitive, protected, or non-public information, in personal cloud storage or other unauthorized services. Cloud services used for City business must meet applicable City security, privacy, and records management requirements.
4. **E-mail and Electronic Communications.** Employees are responsible for retaining e-mail and other electronic communications that constitute City records in accordance with the applicable retention schedule. Not all electronic communications are City records, and routine, transitory, personal, or non-substantive communications may be deleted when they are no longer needed and are not subject to a retention, litigation, audit, investigation, or other legal requirement.
5. **Deleted and Backed-Up Records.** Deleting an electronic record does not necessarily remove all copies of the record from City systems or backups. Employees shall not rely on system backups or deleted-item folders to satisfy records retention requirements and shall not intentionally delete or destroy records that are required to be retained.
6. **GRAMA Requests and Legal Holds.** Electronic records that are subject to a GRAMA request, litigation hold, audit, investigation, or other legal requirement must be preserved and managed in accordance with applicable law and City procedures. Employees shall not delete, alter, or destroy potentially responsive records after receiving notice of such a requirement.

O. THIRD-PARTY AND GUEST ACCESS

1. **Authorized Access.** Vendors, contractors, consultants, and other third parties may be given limited access to City Computer Systems when necessary for authorized City business and approved in accordance with City procedures. Access shall be limited to the systems, information, and duration necessary to perform the authorized work. Third parties with access to City systems shall comply with applicable City security, confidentiality, technology, and acceptable use requirements.
2. **Department Responsibility.** The department responsible for the vendor, contractor, or other third-party shall ensure that access is authorized, limited to the appropriate scope, and removed when it is no longer needed. The department shall

INFORMATION TECHNOLOGY

Revised September 2026

SECTION: 12

maintain a record of third parties authorized to access City Computer Systems and provide that information to the IT Department or other City officials upon request.

3. **Guest Access.** Guests and vendors who need Internet access may use City-approved guest networks or services. Guest access does not provide access to secured City networks, systems, applications, or non-public City information unless specifically authorized.
4. **IT Oversight.** The IT Department may establish access requirements and may restrict, monitor, suspend, or terminate third-party access at any time to protect City systems and information or address security concerns.

P. REPORTING VIOLATIONS

Employees are encouraged to promptly report suspected violations of this policy to their immediate supervisor. If the concern involves the employee's supervisor, the employee may report it to the department head, the Human Resource Director, or the Mayor. Reports will be handled as confidentially as reasonably possible, consistent with the need to investigate and address the concern.

Q. PENALTIES

Violations of this Section may result in disciplinary action in accordance with Tooele City's disciplinary policies, up to and including termination of employment, and may result in revocation of system access, civil liability, or criminal prosecution, as applicable.