COMPUTER SYSTEMS, INTERNET,
AND ELECTRONIC MAIL (E-mail)
Revised June 2022

SECTION: 12

A. APPLICABILITY & DISCLAIMER

1. This policy has been developed to:
    a. Provide for efficient operation of Tooele City's comprehensive computer systems;
    b. Help maintain the integrity of the City's computer systems; and,
    c. Provide guidelines to employees.
2. Due to changes in technology and harmful viruses and programs, Tooele City reserves the right to announce temporary or immediate changes to this Section.

B. DEFINITIONS

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

1. Access to or accessing – opening or searching for material that the employee knew or should have known what the material contained.
2. Computer systems – all hardware, software, computers, laptop computers, tablets, networks, computer hard drives, electronic records, files, disks, Internet access, portable electronic devices, mobile and smart phones, radios, electronic mail (e-mail) systems, social media, equipment, other technological devices, and stored data, including electronic communications and records, on those devices. Computer systems also includes cloud-based or remote systems contracted with Tooele City to be used for City business.
3. Electronic records – all data and records created, stored, deleted, or used on the City's computer systems or personal devices. This includes, but is not limited to, e-mail, computer files, deleted records, data on personal devices used for City business, and social media.
4. Government Records Access and Management Act (GRAMA) - the records law for the State of Utah. GRAMA defines what a record is and establishes the criteria for accessing government records.
5. IT or IT Department – City staff members assigned to Information Technology (IT) Department or provided with duties in support of the IT Department.
6. Social media – all means of communicating or posting information or content of any sort on the Internet, including employees' own or other web log or blog, journal or diary, personal website, social networking or affinity website, web bulletin board or chat room.

C. PROPERTY OWNERSHIP, PRIVACY, & MONITORING

1. The City's computer systems are City property provided to facilitate City business.

2. Employees have no expectation of privacy in use of the City's computer systems. Any use or communications, whether City-related or personal, may be monitored and reviewed by the City or designee at any time. The City is authorized, but not obligated, to monitor and review employee use or communications.

3. The use of computer systems is subject to guidelines and rules as outlined further in this Section.

4. When necessary to conduct City business or as permitted or required by law, the City may disclose the contents of and copy data from any component of the City's computer systems, without the employee's consent.

D. HARDWARE, SOFTWARE & LICENSES

1. The City has invested significant time and money to secure its computer systems from intrusion of harmful viruses and programs. Some hardware is not compatible with the City's computer systems. Employees may not use or install software or hardware without approval from the IT division.

2. The City purchases, owns, and administers the hardware, software, and licenses installed on City computer systems. Employees may not rent, copy, or loan the software, licenses, or documentation.

3. Requests for new hardware or software are submitted to the department head for approval. Each department head discusses such requests with the IT division for compatibility, pricing, and other recommendations.

4. To maintain the integrity of the City systems and license agreements, employees shall not install City-owned software for personal use or on employee-owned devices without approval from their department head and the IT division (refer to Section H).

E. PASSWORDS & COMPUTER SYSTEMS SECURITY

1. **Importance of Strong Passwords & Systems Security -** The data employees work with may be classified as private or protected by law. As such, every employee of Tooele City is a data steward, a protector of information others have entrusted to the City. If a non-authorized individual or entity gains access to City systems it can result in loss of information, theft/release of private or protected information, system unavailability, and other damage including erosion of public trust.

2. **Setting Passwords/Password Requirements -** Passwords are the first level of defense in protecting data and our computer systems. A memorable and strong

password usually consists of a phrase with changed characters. For example, the phrase "This May Be One Way To Remember!" could have a matching password like: "TmB1w2R!" or "Tmb1W>r~" or some other variation (do not use this example). Using a variation of the full sentence as a password is recommended as it is longer and harder to hack. Employees are required to establish strong passwords that as a minimum, meet these requirements:

a. Length of password must be longer than 8 characters.
b. Passwords must be changed every 180 days. Some departments may require passwords to be changed every 90 days.
c. Passwords must include at least 3 of the following:
   (1) Uppercase Letters
   (2) Lowercase Letters
   (3) Numbers
   (4) Symbols
d. Passwords may not contain any part of the following:
   (1) Employee's personal identity information (DOB, name, address, family members, pets names, etc.)
   (2) The words Tooele or City
   (3) Employee's position or job title
e. New passwords must not include the old password with minimal changes (i.e. password1 -> password2).
f. Do not use the same password across multiple logins unless directed to by IT (i.e. using the same password to login to the network as the password for a department specific software system or website).
g. Passwords established for work purposes may not also be used for personal passwords (i.e. do not use work passwords for personal bank account, a home computer, or other personal access).
h. Passwords stored in browsers (such as autofill or "save password prompts") are considered insecure and are at risk of exposure. Employees are advised to utilize a password storage program approved by the IT Department such as LastPass or MyGlue to minimize exposure of City credentials.
i. Devices equipped with pin codes or passcode (smart phones, tablets, or other devices) that access ANY City data are required to have a pin code or passcode set.
j. Passwords must be kept secured. Example:

   (1) **Not Secured**. Password is written on sticky notes or any other similar physical item attached to the employee's desk, computer, or other easily accessible location; password is written in a notebook with other passwords and login information and stored in a desk drawer accessible

to other employees; password is stored in a web browser that has not been secured by a storage program approved by the IT department.

If an employee is having issues remembering passwords, contact IT for suggestions on a secure password manager such as Keepass which allow users to store passwords in a highly protected space.

(2) **Secured**. Password is maintained in a secure password manager system such as Keepass which allow users to store passwords in a highly protected space electronically; password is written down and stored in a locked drawer where others don't have access to it and others are unlikely to know what it is (i.e. a book that says "passwords or login info" is not secure); password and username are not written down or stored together; password is noted on a personal device with a pin or secure access and does not have any identification as to the website, system, login, etc. that it belongs to (i.e. my phone has a simple note in it "Qr$%2lrpr" and nothing else & my phone has a pin number to get into it).

3. **Sharing of Passwords / Password Requests -**
   a. Passwords are unique to individual employees and group passwords are not in line with Tooele City's IT security standards. If multiple employees need access to the same data, contact IT.
   b. Never, under any circumstances should passwords be shared with an outside vendor. Any outside vendor request must be referred to IT for a temporary password.
   c. There may be times where IT will need employee's passwords to troubleshoot an issue. IT will never ask an employee for his/her password over a phone call, email, or text message. If a password is provided to IT, employees will be required to change it once IT is finished with the ticket.
   d. Be aware of scams and phishing attempts. If you are concerned that your password may have been compromised, contact the IT department as soon as possible to get assistance with resetting passwords.

4. **Exceptions** – Tooele City may utilize software, cloud-based, or similar external systems where their password programming does not meet the above requirements (i.e. pin number is used, doesn't reset, etc.). The IT department should be consulted to identify the potential security risk and provide best practice recommendation.

F. PERSONAL USE – ALLOWED & PROHIBITED

Tooele City's computer systems, in general, may not be used for personal use. Tooele City does recognize that incidental/occasional personal use may occur while working and such incidental/occasional use is allowed, provided it is not for one of the following:

1. Any illegal activity;
2. Pornographic material;
3. Classified ads for personal interests;
4. Potential SPAM generators;
5. Downloading, copying, or pirating software or electronic files that are copyrighted or without authorization;
6. Use for personal gain such as business ventures, solicitations, etc.;
7. Use to endorse, support, oppose or contradict any social issue, cause or religion;
8. Introducing malicious software onto the City's network and/or jeopardizing the security of the City's electronic communications systems;
9. Use that violates Tooele City's Equal Employment Opportunity, Anti-Harassment and Anti-Retaliation polices;
10. Use that discourages productivity such as group or mass mailings of jokes, chain letters, and non-business-related photographs, Internet surfing, and computer games;
11. Accessing or participating in non-work related chat rooms;
12. Downloading screen savers, music, movies, or other non-work related material;
13. Use by family or non-City employees;
14. Use of network sniffer or hacker software;
15. Any other use that may compromise the integrity of the City computer systems.

G. EMAIL GUIDELINES

1. E-mail should be used with the same level of professionalism as any other written communication.

    a. E-mail could be classified as a public document and disclosed.
    b. E-mail should not be used to transmit sensitive materials, such as personnel decisions and other similar information that may be more appropriately communicated in writing or personal conversation.
    c. E-mail messages can be forwarded without the express permission of the original author.
    d. E-mails are relatively insecure communications and can be easily intercepted and viewed. Employees should use caution in the transmission and dissemination of messages outside of the City.
    e. E-mail should not be used to transfer large files. Contact IT for other means of transferring large files.

f. E-mail signatures are expected to follow the template provided by the City.

2. Passwords should not be communicated through e-mail.

3. E-mails often include links to websites or advertisements that are set up with the intent to trick users into installing software that will hijack a computer. Employees are reminded to be very cautious of e-mails opened with City computers and to NOT click on the link or open attachments of suspicious e-mail.

4. Tooele City understands that employees may involuntarily receive or inadvertently open e-mails containing material that is listed as prohibited.

H. USE OF PERSONAL DEVICES

1. Department head permission is required when employees use personal devices, such as phones, tablets, IPads, etc., for work-related duties. Personal devices must be secured consistent with Section E above. If the personal device is stolen or lost, employees are to contact IT and their department head immediately.

2. The employee is ultimately responsible for proper operation and functionality of any personal devices. The IT division may assist the employee with personal devices used for City business with the understanding that they are doing so in good faith and within their own level of expertise. The City is not responsible for the functionality of the personal device even if worked on by the IT Department. Circumstances may necessitate resetting devices and may result in data loss. Employees are responsible for backing up or securing their data prior to requesting assistance from IT.

3. Employees are reminded that using personal devices for City business may subject those devices to search and discovery in legal proceedings which may require the device to be taken for a period of time. The City is under no obligation to provide a replacement.

4. See M below for additional information regarding storage & retention of electronic records including cloud storage.

I. CITY WEBSITES

City websites, including tooelecity.org and specific department websites, may be used to enhance communications subject to the following rules and guidelines:

1. All Tooele City websites are to be approved by the Mayor.

2. Examples of prohibited postings include:

a. Classified advertisements;
b. Advertisements that endorse, support, oppose or contradict any social issue, cause or religion (unless they are local events open to the public); or
c. Commercial business advertisements that are not of global public interest or are not for City-sponsored projects such as downtown revitalization or sponsors for community activities.

3. Only employees designated as webmasters are authorized to post information to City websites.

4. All content created or posted on a City social media site belong to Tooele City.

5. The Mayor makes all final decisions about information posted to City websites.

J. CITY USE OF SOCIAL MEDIA

City social media, including the City's Facebook page and specific department social media efforts, may be used to enhance communications with citizens and program participants subject to the following rules and guidelines:

1. All Tooele City social media sites are approved by the Mayor.

2. Tooele City social media sites are generally used for:

   a. Marketing/promotional channels which increase the City's ability to broadcast its messages to the widest possible audience;
   b. Public information updates; and
   c. The dissemination of time sensitive information (i.e. emergency information).

3. Content posted to Tooele City social media sites are expected to portray a professional image of Tooele City.

4. Content should also be made available on the City's main website whenever possible. Content posted to the City social media sites should contain links directing users back to the City's official website for in-depth information, forms, documents, or online services necessary to conduct business with Tooele City.

5. City social media sites may be used only for communication of City-related information and may not be used for personal purposes.

6. Examples of prohibited articles and comments include:

   a. Comments in support of or opposition to political campaigns or ballot measures;
   b. Profane or obscene language or content;

c. Content that violates Tooele City's Equal Employment Opportunity, Anti-Harassment and Anti-Retaliation policies, including sexual content or links to sexual content;
d. Content that markets or promotes other businesses, unless such business is a sponsor of a City event or program, or is a business partner with Tooele City for public services;
e. Conduct or encourage illegal activity;
f. Information that may tend to compromise the safety or security of the public or public systems; or
g. Comments not typically related to the particular social media article being commented upon, including random or unintelligible comments.

7. The guidelines described above should be displayed to users or made available by hyperlink.

8. Tooele City reserves the right to restrict or remove any content that is deemed to be in violation of this Section, has the potential to bring discredit to the City, violates any law, or is contrary to the public interest. A copy of any content removed based on these guidelines must be retained, including the time, date, and identity of the poster when available for a period of time determined by the City records officer consistent with state retention schedules.

9. All content created or posted on City social media sites belongs to Tooele City.

10. The City webmaster either collects and maintains all passwords to approved social media sites, or has administrative access to these sites. Passwords follow the password policy in this Section.

11. Final decisions about information posted to social media are approved by the Mayor.

K. EXCEPTION TO CITY USE OF SOCIAL MEDIA

Law enforcement personnel and legal staff may engage in use that is listed as prohibited when such use is necessary to perform their law enforcement and legal duties and he/she has received advance approval from his/her supervisor. It is recommended that supervisors provide the IT Department with notice of authorized use.

L. EMPLOYEE PERSONAL USE OF SOCIAL MEDIA

Employees' personal use of social media may create workplace implications. Therefore, the following guidelines and reminders are provided to employees:

1. **Workplace Implications** – The same principles and guidelines found in Tooele City's policies and procedures apply to social media activities. Conduct that adversely affects job performance, the workplace, the performance of fellow

associates or otherwise adversely affects members, citizens, suppliers, people who work on behalf of Tooele City may be job-related. Employees are responsible for what they post online and are encouraged to consider some of the risks and rewards that are involved with social media activities.

2. **Know Policies and Procedures** – Employees are expected to carefully read these guidelines and the City's Personnel Policies and Procedures giving special attention to EEO, No-Harassment & No-Retaliation, and Disciplinary Sections to ensure that postings are consistent with these policies. Employees are specifically expected to refrain from social media activities that reasonably could be viewed as malicious, obscene, and threatening or intimidating, that disparage citizens, members, associates or suppliers, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law.

3. **Be Respectful** – Employees should be fair, courteous, and respectful to fellow employees, citizens, suppliers or people who work on behalf of Tooele City.

4. **Consider Available Internal Resources to Resolve Workplace Complaints** – Workplace complaints are more likely to be resolved by speaking directly with co-workers or by utilizing the City's internal grievance procedure than by posting complaints to a social media outlet.

5. **Be Honest and Accurate** – Employees are expected to convey a true and accurate impression of the facts and circumstances, to be honest, and to be accurate when posting information or news, and if a mistake is made, to correct it quickly.

6. **Confidentiality and GRAMA** – Employees are expected to maintain the confidentiality of private, confidential, and protected information. Employees may not post internal reports, other internal business-related confidential communications or records that have not been obtained pursuant to GRAMA.

7. **Disclosure** – Express only personal opinions. Employees may not represent themselves as a spokesperson for Tooele City. If Tooele City is a subject of the content being created, employees should be clear and open about the fact that they are an employee and make it clear that the views do not represent those of Tooele City, fellow associates, members, citizens, suppliers or people working on behalf of Tooele City. If employees do publish a blog or post online related to their work or subjects associated with Tooele City, they must make it clear that they are not speaking on behalf of Tooele City. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of Tooele City."

8. **Permanent Records** – The Internet archives almost everything; therefore, even deleted postings can be searched. Employees are reminded that their social media activities can become permanent records. Often times messages on social media reach a broader audience than was intended when the message was posted and these messages may be difficult to edit or retract once posted.

M. STORAGE & RETENTION OF ELECTRONIC RECORDS

1. Department heads set standards for retention of electronic records. Individual department policy should follow the Utah Municipal General Records Retention Schedule.

2. Cloud services should not be used to store data unless approved by IT and the employee's supervisor. Sensitive data should be encrypted before being stored on Cloud services. Cloud services should not be used on personal devices unless it is password protected, and, if it contains sensitive information, that information should be encrypted. Other Cloud services should be reviewed with IT for approval and security just like any other application.

3. Electronic records generated or received on the City systems may be public records and may be subject to public inspection. This includes, but is not limited to:

   a. E-mails;
   b. Social media;
   c. Deleted files;
   d. Data on personal devices used for City business; and,
   e. City's computer systems.

4. Public requests for electronic records will be handled in compliance with GRAMA.

5. Deleted records, including deleted e-mail messages from a workstation mailbox, might not be deleted from the central computer systems. Records may be stored on the computer's back-up system for an indefinite period.

6. Employees should archive all official and/or substantive e-mail messages, as they would paper letters and memoranda. Casual, personal, non-substantive, advertisements, and other such e-mail messages should be deleted as soon as possible after receiving them.

N. SOFTWARE VENDORS, GUESTS, AND CONTRACTORS

1. When software vendors are visiting or accessing Tooele City and request a need to access the City's computer system, they may be granted limited access to the City

network to administer, upgrade, or update their software. This shall be done under careful guidance of IT.

2. Guests, sales agents, and other non-City business related access can be allowed to use the Internet through a special visitor logon account to prevent access to City data, network, and equipment. Also, credentials may be shared for the use of non-internal Internet access, utilizing a wireless access point, by contacting an IT employee, when service is available. No one should connect to the City's network without IT permission.

3. Contractors may be granted the right to access the City's computer systems, with the Mayor's approval. Contractors are required to abide by this policy regarding acceptable use guidelines.

O. REPORTING VIOLATIONS

Employees should report violations of this policy to their immediate supervisor, or, if the violation is allegedly being committed by the supervisor, the employee may choose to report the violation to the department head, the human resource director, or the Mayor. To the extent possible, reports will be handled with confidentiality.

P. PENALTIES

Violations of this Section may be considered sufficient cause for disciplinary action in compliance with Tooele City's disciplinary policies, up to and including termination. Employees may be held responsible for any damages caused by unauthorized software or viruses they introduce into the computer system. In addition, violations of this Section or misuse of the e-mail, Internet system, or social media may be referred for criminal prosecution if warranted.