**SECTION:** **AGENCY PROPERTY**

**POLICY:** Computer and Internet Use **EFFECTIVE DATE:** insert date adopted

(Electronic Media) Policy

**STATEMENT OF PURPOSE:**

Employees have access to one or more forms of electronic media and services (computers, email, telephones, voicemail, fax machines, external electronic bulletin boards, wire services, the Internet, online messaging systems, online meetings and calls, and other services).

The City encourages the use of these media and associated because they make communication more efficient and effective, and because they are valuable sources of information. However, electronic media and services provided by the City are City property, and their purpose is to facilitate City business.

With the rapidly changing nature of electronic media, this policy cannot lay down rules to cover every possible situation. Instead, it expresses the City’s rules and sets forth general principles to be applied to the use of electronic media and services.

This policy is intended to fulfill the requirements of SB 1893 which prohibits the social media service TikTok or any successor application or service developed or provided by ByteDance Limited, or any entity owned by ByteDance Limited on City owned or leased devices.

**DEFINITIONS:**

This policy has included the Definitions section in the Procedures section.

**APPLICABILITY:**

This policy applies to employees of the City.

**PROCEDURES:**

The following procedures apply to all electronic media and services that are accessed on or from City premises, accessed using City computer equipment, or via City-paid access methods, and/or used in a manner which identifies the individual with the City.

1. Usage
2. Electronic media may not be used for knowingly transmitting, retrieving or storage of any communications of a discriminatory or harassing nature, or which are derogatory to any individual or group, or which are obscene or X-rated communications, or are of a defamatory or threatening nature, or for ‘chain letters,’ or for any other purpose which is illegal or against City policy or contrary to the City’s interest.
3. Electronic media and services are primarily for City business use. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable—as is the case with personal phone calls. However, employees need to demonstrate a sense of responsibility and may not abuse the privilege.
4. Monitoring
5. The city routinely monitors usage patterns for both voice and data communications (e.g., number called, or website accessed; call length; times of day when calls were made; used computer application; computer screen copies, etc.). The City also reserves the right, in its discretion, to review any employee’s electronic files and messages and usage to the extent necessary to ensure that electronic media and services are being used in compliance with the law and with this and other City policies.
6. Employees should therefore not assume electronic communications and their actions on work computers are totally private and confidential and should transmit highly sensitive information in other ways.
7. Security
8. Employees must respect the confidentiality of other people’s electronic communications and may not attempt to read, ‘hack’ into other systems or other people’s logins, or ‘crack’ passwords, or breach computer or network security measures, or monitor electronic files or communications of other employees or third parties except by explicit direction of City management. No email or other electronic communications may be sent which attempt to hide the identity of the sender or represent the sender as someone else or from another City.
9. The City will manage all City-owned or leased mobile devices by implementing the security measures listed below:
   1. Restrict access to “app stores” or unauthorized software repositories to prevent the installation of unauthorized applications.
   2. Maintain the ability to remotely wipe non-compliant or compromised mobile devices.
   3. Maintain the ability to remotely uninstall unauthorized software from mobile devices.
   4. Maintain any other measure necessary to insure the security of the City’s systems.
10. Congestion
11. Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.
12. Copyright
13. Anyone obtaining electronic access to other Citys’ or individuals’ materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner or a single copy for reference use only.
14. Networks
15. Any messages or information sent by an employee to one or more individuals via an electronic network (e.g., bulletin board, on-line service, or internet) are statements identifiable and attributable to our City. While some users include personal ‘disclaimers’ in electronic messages, it should be noted that there would still be a connection with the City, and the statement might still be legally imputed to the City. All communications sent by employees via a network must comply with this and other City policies and may not disclose any confidential or proprietary City information.
16. Prohibited Applications
    * The City will identify, track, and manage all government-owned or –leased devices including mobile phones, tablets, laptops, desktop computers, or any other internet-connected devices to:
      1. Prohibit the installation of a covered application including the social media service TikTok or any successor application or service developed or provided by ByteDance Limited, or any entity owned by ByteDance Limited.
      2. Prohibit the use of a covered application.
      3. Remove a covered application from a City-owned or –leased device that was on the device prior to the passage of S.B. 1893 (88th Leg., R.S.).
17. Network services and World Wide web sites can and do monitor access and usage and can identify at least which City—and often which specific individual—is accessing their services. Thus, accessing a particular bulletin board or website leaves City-identifiable electronic ‘tracks’ even if the employee merely reviews or downloads the material and does not post any message.
18. Discipline
19. Any employee found to be abusing the privilege of City-facilitated access to electronic media or services will be subject to corrective action up to and including termination of employment and/or risk having the privilege removed for him/herself and possibly other employees.

**COMPUTER AND INTERNET USE POLICY**

**ACKNOWLEDGMENT**

Employee Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Position:

Date of Receipt of Computer and Internet Use Policy:

I acknowledge and agree that:

1. I have received a copy of the City Computer and Internet Use Policy;
2. I have read the Computer and Internet Use Policy in its entirety and fully understand the provisions contained therein; and
3. I agree to abide by the provisions contained in the Computer and Internet Use Policy.

Employee’s Signature

Employee’s Name (Printed)

Date