***[Organization Logo]***

Address, City, State, Zip Code Phone XXX.XXX.XXXX / Fax XXX.XXX.XXXX

**[Organization Name] Employee Agreement on Responsible Use of Electronic Resources**

The [Organization Name] recognizes the value of computers and other electronic resources to improve public service and enhance the administration and operations of its municipal departments. To this end, the [Organization Name] encourages the responsible use of computers, computer networks, including the Internet, and other electronic resources in support of the mission and goals of the [Organization Name].

Recognizing that the Internet is an unregulated, global platform where information access is often beyond control, the City Council has adopted this policy, in compliance with Senate Bill 1893 of the 88th Texas Legislature, to provide essential guidance on the responsible use of electronic resources. This policy framework is designed to protect the integrity of City-owned equipment and City-affiliated organizations, maintaining security while empowering employees to effectively serve the community.

*[Organization Name] Rights and Responsibilities*

It is the policy of the [Organization Name] to maintain an environment that promotes ethical and responsible conduct in all online network activities by staff and authorized users. It shall be a violation of this policy for any employee or other individual to engage in any activity that does not conform to the established purpose and general rules and policies of the network. Within this general policy, the [Organization Name] recognizes its legal and ethical obligation to protect the well-being of authorized users in its charge. To this end, the [Organization Name] retains the following rights and recognizes the following obligations:

1. To log network use and to monitor fileserver space utilization by users, and assume no responsibility or liability for files deleted due to violation of fileserver space allotments.
2. To remove a user account on the network.
3. To monitor the use of online activities. This may include real-time monitoring of network activity and/or maintaining a log of Internet activity for later review.
4. To provide internal and external controls as appropriate and feasible. Such controls shall include the right to determine who will have access to [Organization Name]-owned equipment and, specifically, to exclude those who do not abide by the [Organization Name]'s acceptable use policy or other policies governing the use of school facilities, equipment, and materials. [Organization Name] reserves the right to restrict online destinations through software or other means.
5. To provide guidelines and make reasonable efforts to train staff and authorized users in acceptable use and policies governing online communications.

*Staff Responsibilities*

1. Staff members who supervise authorized users, control electronic equipment, or otherwise have occasion to observe the authorized user use of said equipment online shall make reasonable efforts to monitor the use of this equipment to assure that it conforms to the mission and goals of the [Organization Name].
2. Staff should make reasonable efforts to become familiar with the Internet and its applications to ensure effective monitoring, guidance, and support in their roles.

*User Responsibilities*

1. Use of the electronic media provided by the [Organization Name] is a privilege that offers a wealth of information and resources for improving workplace processes. Where it is available, this resource is offered to staff, authorized users, and other patrons at no cost. In order to maintain the privilege, users agree to learn and comply with all of the provisions of this policy.

*Acceptable Use*

1. All use of the Internet must support operational and administrative objectives consistent with the mission and goals of the [Organization Name].
2. Proper codes of conduct must be followed in all electronic communications. Sharing personal information in public forums or discussion groups is inappropriate. When using email, employees should exercise extreme caution in disclosing any personal or sensitive information.
3. Network accounts are to be used only by the authorized owner of the account for the authorized purpose.
4. All communications and information accessible via the network should be assumed to be private property.
5. Employees are expected to use their best discretion when subscribing to mailing lists or bulletin boards, ensuring that subscriptions align with City goals and professional standards.
6. Mailing list subscriptions will be monitored and maintained, and files will be deleted from the professional mail directories to avoid excessive use of fileserver hard-disk space.
7. From time to time, the [Organization Name] will make determinations on whether specific uses of the network are consistent with the acceptable use practice.

*Unacceptable Use*

1. Sharing personal information about another person, including home address and phone number, is strictly prohibited except when necessary for work-related purposes and authorized by City policy.
2. Any personal use of the network for commercial or for-profit purposes is prohibited.
3. Excessive use of the network for personal business shall be cause for disciplinary action.
4. Any use of the network for product advertisement or political lobbying is prohibited.
5. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the network.
6. No use of the network shall serve to disrupt the use of the network by others. Hardware and/or software shall not be destroyed, modified, or abused in any way.
7. Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited.
8. Hate mail, chain letters, harassment, discriminatory remarks, and other antisocial behaviors are prohibited on the network.
9. The unauthorized installation of any software, including shareware and freeware, for use on [Organization Name] computers is prohibited.
10. The [Organization Name] strictly prohibits the installation or use of unauthorized applications, including but not limited to *TikTok, CapCut, Hypic, Xigua Video, Ulike*, and other applications developed by ByteDance, on any City-owned or -operated devices and networks. These applications pose potential security risks, including data privacy concerns, that may compromise the integrity of City information systems. Employees are expected to adhere to this policy, and any unauthorized use may result in disciplinary action, including revocation of access privileges and/or other appropriate measures.
11. Use of the network to access or process pornographic material, inappropriate text files (as determined by the system administrator or building administrator), or files dangerous to the integrity of the local area network is prohibited.
12. The [Organization Name] network may not be used for downloading entertainment software or other files not related to the mission and objectives of the [Organization Name] for transfer to a user's home computer, personal computer, or other media. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files not directly related to the instructional and administrative purposes of the [Organization Name].
13. Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner is prohibited, except that duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC).
14. Use of the network for any unlawful purpose is prohibited.
15. Use of profanity, obscenity, racist terms, or other language that may be offensive to another user is prohibited.
16. Establishing network or Internet connections for live communications, such as voice or video through platforms like Teams and Zoom, is permitted for work-related or educational purposes. However, employees should ensure that such use aligns with City policies and does not disrupt services.

*Disclaimer*

1. The [Organization Name] cannot be held accountable for the information that is retrieved via the network.
2. Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. System administrators have access to all mail and will monitor messages. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.
3. The [Organization Name] will not be responsible for any damages you may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by our own negligence or your errors or omissions. Use of any information obtained is at your own risk.
4. The [Organization Name] makes no warranties (expressed or implied) with respect to:
   * the content of any advice or information received by a user, or any costs or charges incurred as a result of seeing or accepting any information; and
   * any costs, liability, or damages caused by the way the user chooses to use his or her access to the network.
5. The [Organization Name] reserves the right to change its policies and rules at any time.

*User Agreement (to be signed by all authorized users)*

*I have read, understand, and will abide by the above Acceptable Use Policy when using computers and other electronic resources owned, leased, or operated by the [Organization Name]. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, disciplinary action may be taken, and/or appropriate legal action may be initiated.*

**Signature:** **Date:**

**Printed Name:**