CITY OF DECATUR Texas	CITY OF DECATUR PERSONNEL POLICY		
Chapter 05	**Conduct**		
Section 11	**Acceptable Use Policy**		
Revised By:	**Nate Mara, City Manager**	**Revised Date:**	**December 22, 2025**
Approved By:	**Nate Mara, City Manager**	**Effective Date:**	**January 1, 2026**

05.11 Acceptable Use Policy

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources owned or leased by the City of Decatur in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

The City of Decatur provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the City against damaging legal issues. This acceptable use policy applies to all employees, contractors, consultants, temporary, and other workers at the City of Decatur including all personnel affiliated with third parties. Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment. A violation of this policy by a temporary worker, contractor, or vendor may result in the termination of their contract or assignment with the City of Decatur.

A. **Good Judgment**
   a. Employees are responsible for exercising good judgment regarding appropriate use of City resources in accordance with City policies, standards, and guidelines.
   b. City resources may not be used for any unlawful, unethical, or otherwise prohibited purposes.
   c. The restrictions outlined in this policy are not to be considered an exhaustive list of all possible infractions of this policy.
   d. Common sense should be used for any activity not strictly prohibited in this policy.

B. **Personal Use of City Equipment**
   a. The City's information assets and resources are made available to help employees perform their job duties and are not intended for personal use.
   b. The City recognizes that under certain circumstances the employee's occasional use of City telephones, computers, facsimile, e-mail, copiers, Internet service, and similar resources for personal use may be necessary or beneficial to the City.

c. The City may establish separate policies governing the use of specific equipment.
d. An employee that demonstrates excessive use of City equipment for personal use shall be subject to disciplinary action up to termination.

C. **Cybersecurity Training**

All employees who are given access to the City of Decatur's technology resources are required to complete an annual cybersecurity training program that has been certified by the Texas Department of Information Resources (DIR) as mandated by the State of Texas. Failure to complete the course by its due date may result in disciplinary action.

D. **Personal Responsibility for System Accounts**

a. Employees are responsible for the security of data, accounts, and systems under their control.
b. An employee should keep passwords secure and should not under any circumstances share account or password information with anyone, including other personnel, family, or friends.
c. Providing access to an individual's account to another individual, either deliberately or through failure to secure its access, is a violation of this policy.
d. The storage of credentials such as passwords and door codes on City computers or servers, or on paper that is kept at the employee's desk is strictly prohibited.
e. Users should memorize their passwords, write their passwords on paper and keep that paper in a locked drawer or cabinet, or use a password manager that encrypts their entries to store their passwords.
f. Passwords stored on computers in clear text or written in insecure areas such as in a shared office space are susceptible to misuse by unauthorized people and is therefore prohibited.
g. Improper storage of network credentials may result in disciplinary action up to and including termination.
h. These prohibitions also apply to the storage of account credentials for third party services that are used for City business.

E. **Computing Assets**

a. Employees are responsible for ensuring the protection of assigned City assets.
b. Employees should promptly report any theft of City assets to Information Technology.
c. All PCs, laptops, workstations, tablets, and other devices must be secured with a password-protected screensaver with an automatic activation feature of 10 minutes or less.
d. An employee must lock the screen or log off when the device is unattended.
e. Employees are strictly prohibited from interfering with any device management or security system software, including but not limited to, antivirus, content filtering, or remote access software.

f. Employees should be aware that in the case of equipment failure, Information Technology does not perform data recovery. All users are encouraged to use network storage drives for critical files.
g. Network drives are backed up on a daily basis to ensure reliability.

F. **Privacy Restrictions**

a. All activities performed on any City-owned or leased device or personal device connected to the City's network are logged as they are performed.
b. Email correspondence, website visits, downloads, and all other actions carried out using City resources can be viewed by authorized personnel with or without notice to an employee for purposes such as maintenance, security hardening, and auditing. Such logs are considered the property of the City and are not subject to consent from the end user.
c. Emails sent or received on the City's email server and their attachments, files stored on machines, and logs generated by end users on network resources or City-owned or leased equipment are also considered the property of the City of Decatur. Their contents can be accessed and read by authorized personnel for purposes including, but not limited to, the following:
    1. Access by the Information Technology staff during the course of system maintenance or administration;
    2. Access approved by the employee, the employee's supervisor, or senior staff (City Manager, City Attorney, and Department Directors) when there is a business reason to access the employee's files or mailbox. For example, if an employee is absent from the office and the supervisor has reason to believe that information relevant to the City's business is located in the employee's mailbox;
    3. Access approved by the employee's supervisor, the City's Human Resources department, Information Technology, or senior staff when there is reason to believe the employee is using resources in violation of the City's policies;
    4. Access approved by the City's Human Resources department in response to the City's receipt of a court order or request from law enforcement officials for disclosure of an employee's email messages or stored files.

G. **Copyright Restrictions**

a. An employee found to be engaging in theft, corruption, or alteration of any of the City's computer data or programs is subject to discipline, discharge, or criminal prosecution.
b. There may be occasions where employees use City laptops or software at home. This usage must be approved by the employee's supervisor in advance and must be coordinated and approved by the City's Information Technology staff.
c. Use of City equipment and/or software off premises is still covered by this policy.
d. The City prohibits illegal duplication of software and its related documentation.

e. The unauthorized use, copying, or distribution of copyrighted software is a violation of the Digital Millennium Copyright Act (DMCA). Examples of violations include, but are not limited to, the following:
    1. Making extra copies of software for use on other computers unless specifically allowed through a licensing agreement;
    2. Making copies of software available so that they may be used by others;
    3. Obtaining copies of software from others without paying the appropriate licensing fees; and
    4. Unauthorized distribution of software by e-mail.
f. Employees are to be provided, by the City Information Technology staff, appropriately licensed copies of computer software necessary to perform their assigned tasks.
g. To ensure adherence to the DMCA, regular audits will be conducted to search for unauthorized software installed on machines and network servers.
h. Users may be held responsible for any such software found on their machines or in their possession.
i. The unauthorized use of City-owned license keys for license-protected software on personal devices is considered theft (such as installing Microsoft Office on a personal device using the City's license key without written authorization).

H. **Acceptable Uses**
a. Acceptable uses of the City's electronic communication systems are limited to those activities that support reference, research, internal/external communication, and conducting City business in line with the user's job responsibilities.
b. Network users are encouraged to develop uses which meet their individual needs and which take advantage of the City's internal network functions.

I. **Unacceptable Uses**

Unacceptable uses of City-owned or leased electronic communication systems include but are not limited to:

- Using profanity, obscenity, or other language which may be offensive or harassing to other coworkers or third parties;
- Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software;
- Use of City devices for financial gain or business unrelated to the City of Decatur;
- Using systems or installing software/hardware on systems in such a manner as to create a breach of the security of the City's network;
- Seeking employment opportunities outside the City of Decatur;
- Expressing opinions or personal views that could be misconstrued as being those of the City;
- Expressing opinions or personal views regarding management, business, or decisions of the City or other political views;

- Accessing, playing, downloading, or distributing confidential information for which access has not been granted or distribution has not been approved;
- Causing a disruption of service to either the City or its network resources;
- Introducing "rogue devices" on the network (devices for which installation has not been approved by Information Technology);
- Port scanning or security scanning on a production network unless authorized in advance by Information Technology; or
- Using the City of Decatur network for personal use, including, but not limited to, entertainment, social networking (except as required by job function), playing games, and accessing adult content.

J. **Electronic Communications Restrictions**

The following are strictly prohibited:

- Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities and procuring or transmitting material that violates the City of Decatur policies against harassment or the safeguarding of confidential or proprietary information;
- Sending spam via email, text messages, pages, instant messages, voice mail, or other forms of electronic communication;
- Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender;
- Posting the same or similar non-business-related images to large numbers of distribution groups (newsgroup spam);
- Use of a City of Decatur email or IP address to engage in conduct that violates the City of Decatur policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with a City of Decatur email or IP address represents the City to the public; therefore, an employee must exercise good judgment to avoid misrepresenting or exceeding their authority in representing the opinions of the company;
- Using a City-provided email address for personal use, such as personal subscriptions, social media, or other non-business-related accounts.