
# Dallas County Information Technology Acceptable Use Policy

## 1. Scope

The Dallas County Acceptable Use Policy applies to all Users (County employees, elected officials, contractors, subcontractors, part-time and temporary workers, individuals telecommuting, and those who have been granted access to County's electronic and computing devices).

Computing resources include all Dallas County-owned, licensed, or managed hardware and software, data, information, information assets, Dallas County-assigned user accounts, and use of the Dallas County network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Because Dallas County owns the network, this Policy applies to technology administered in all departments and divisions, all computers and devices connected (wired and wireless) to the Dallas County network, and to off-site computers that connect remotely to the Dallas County network services.

This Policy supersedes all other policies on this topic either written or verbal.

## 2. Purpose

This document defines the policy necessary for establishing acceptable and unacceptable practices while carrying out day-to-day job functions within Dallas County work environments.

## 3. Policy

*User IDs and Passwords*

To support the protection of Dallas County confidential information and compliance with various regulatory requirements, all Users will be assigned a unique user ID and password for accessing computer systems and networks.

- Users will select passwords that are not easily guessed nor words found in a dictionary, taking care to choose passwords that contains each of the following: small letters, capital letters, numbers, and a special character.

  Note: A password written on an adhesive note and placed on the desk, keyboard, or monitor is strictly prohibited.

- Users are responsible for any system or network activity generated by their user ID and should not share their passwords with other individuals. If a password must be disclosed, the employee must change it at the next possible opportunity.

*County Issued Devices, and Internet*

Dallas County-issued devices- workstations (i.e., laptops, desktops, tablets, iPads, etc.), cell phones, and the use of Internet system are provided to Users for the purpose of county business. Dallas County-issued devices and Internet system are owned by the County. Additionally, all communications and information transmitted by, received from, or stored in these systems are County records and the sole property of Dallas County. The County reserves the right to monitor its devices, and any messages, attachments, use of electronic mail, and Internet sites on the Internet system, subject to state and federal law. Users of

County-issued devices, and the Internet system may be subject to disciplinary measures and legal consequences if policy violations occur.

Users should limit personal communications during work periods to break periods and lunch periods, whenever possible. Users should note that these personal communications may be subject to monitoring by the County and may become public due to the Public Information Act. There is no expectation of privacy using the County technology resources. Use of any instant messaging services is strictly limited to Dallas County internal communications. Users are required to conduct themselves in a professional manner while using the information technology resources and limit use of technology resources for purposes that are unrelated to County business*. Confidential messages must be handled with extreme care*.

Users should utilize all information technology resources with the same care, judgment and responsibility that they would use when sending letters or memoranda written on County letterhead. Extreme care must be taken when posting any information on commercial online systems, social media or the Internet because of the potentially broad distribution and access to such information. Sending information to non-authorized entities or posting on an unauthorized website is strictly prohibited.

To protect the integrity of the communications systems and to ensure proper County business-related use, Dallas County reserves the right, without notice, to:

- Limit or restrict any individual's use
- To inspect, copy, remove or delete any of its systems or data
- To access user's voicemail, Internet access, email and data files

*Appropriate Use*

County Workforce members are encouraged to only use County-issued devices, and the Internet to further the goals and objectives of Dallas County. The types of activities that are encouraged include:

- Communicating with fellow employees, business partners of the County, or constituents within the content of an individual's assigned responsibilities.
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
- Participating in educational or professional development activities.

*Inappropriate Use*

Users are prohibited from using the information technology resources for any unauthorized or unlawful purpose, including but not limited to the following:

- Use of email, phone, and internet for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g., spreading of computer viruses).
- Users of the information technology resources are strictly prohibited from delivering a message that is harassing or offensive based on race, color, creed, sex, national origin, citizenship, sexual

orientation, age, ancestry, marital status, physical disability, mental disability, or any other consideration made unlawful by federal or state law.

- Users should refrain from accessing non-business-related internet sites during regular business hours. Employees should limit personal use accessing the internet to lunch periods or break periods whenever possible. Internet use will not be allowed to interfere in normal business operations.
- Users must respect all copyrights and licenses to software and other online information, and may not upload, download, or copy software or other material through the communications systems without clearance from the Office of Information Technology.
- Users are prohibited from the use of streaming video or audio due to the large amount of bandwidth required for those applications unless the job function requires such services.
- Users are prohibited from using Dallas County equipment to share any Dallas County data, which includes pictures or videos of county employees in the performance of their duties, on Facebook, Instagram, TikTok, Box.com, Dropbox, Jumpshare, ShareFile, external OneDrive, iCloud, and any other file sharing service.
- Users must not alter, copy, transmit, or remove County information, proprietary software or other files without proper written authority from the Office of Information Technology. This does not include transfer of data, copying, transmittal, or removal that is required by your position or has been requested by a Department Head or Elected Official.
- Users must not auto or SMTP forward Dallas County received emails to any outside or external, non-Dallas County, destination.
- Users are prohibited from reading, copying, recording, or listening to messages and information delivered to another person's email and voice mailboxes without proper authorization. Anyone who receives an electronic communication for which she or he is not the intended recipient must immediately inform the sender that the message was sent improperly and delete the message from his or her email and voice mailbox.
- Users are prohibited from sending, saving, or viewing offensive, adult oriented, or sexual material. This does not include bona fide law enforcement investigations conducted by County employees.
- Users are prohibited from storing or transmitting on Dallas County computers, voicemail, email, or telephone systems content which may reasonably be considered offensive or harassing to any other User or County employee. Offensive material includes, but is not limited to, sexual comments, jokes or images, racial slurs, gender-specific comments, or any comments, jokes or images that would offend or degrade someone based on their race, color, religion, sex, sexual orientation, age, national origin or ancestry, physical or mental ability, sexual orientation, as well as any other category protected by federal or state law.
- Users who are County employees shall not perform unauthorized searches of other Users' email, instant messaging, voicemail, cellular telephone, or network use without written authorization from the Chief Privacy Officer or an attorney within the Civil Division of the District Attorney's Office. This section does not apply to the IT Security Team performing their job functions.

**Instant Messaging**

Use of external Instant Messaging (IM) software is prohibited. This means the access to or use of

external IM services such as FB Messenger, WhatsApp, WeChat, Telegram, Yahoo, Line, MSN, Viber, and the like, from a Dallas County device or system is prohibited.

The same policies and guidelines that are in place for email are also applicable to the IM system.

**Software**
The download of any software, which is not approved or for which prior approval to do so has not been granted is prohibited.

At no time can software be downloaded to bypass the County's firewalls or other protective systems. The Office of Information Technology reserves the right to audit and remove any and all unauthorized software installed on a County asset.

**Virtual Private Networking (VPN)**
The use of unauthorized VPN providers or VPN tools is prohibited. Authorized Virtual Private Network (VPN) or remote access is available for Users that are issued a portable device. The appropriate documentation must be submitted for vendors requiring VPN access through the IT ServiceDesk. Personal computers of Users will not be provisioned for VPN access.

**Copyrighted Material**
Users may not copy and distribute copyrighted material (e.g., software, database files, documentation, articles, graphics files, or downloaded information) through the email system or by any other means unless you have confirmed in advance with the Civil Division of the District Attorney's Office that the County has the right to copy or distribute the material. Failure to observe a copyright may result in disciplinary action by Dallas County as well as legal action by the copyright owner.

*Acceptable Use Acknowledgement*
Each User will be presented with a login banner and will be required to acknowledge the Acceptable Use guidelines before being prompted with username and password.

Users are responsible for the content of all text, audio, or images that he/she places or sends over the County's data networks. Users may access only files or programs, whether computerized or not, that they have authorization to use.

## 4. Periodic Reviews and Audits
This Policy will be reviewed and updates on an annual basis.

## 5. Enforcement and Exception Handling
All the Users must follow this Policy. Failure to comply with the Criminal Justice Information Policy (CJIS), Dallas County Code, other applicable data privacy regulations, this Policy and Dallas County Security Policies can result in a loss of access and disciplinary actions, up to and including termination of employment, contracts, or other relationships. Additionally legal action may also be taken in response to violations of applicable regulations and laws.

Requests for exceptions to this Policy should be submitted to the ServiceDesk and routed to the Security Team. Exceptions will be permitted only upon receipt of written approval from both the Dallas County Chief Information Officer and Chief Privacy Officer.

## 6. References

| |
|---|
| NIST SP 800-53 Moderate Baseline Control Objectives |
| FBI Criminal Justice Information Services (CJIS) |
| OCR Health Insurance Portability and Accountability Act – Privacy Rule |
| Payment Card Industry-Data Security Standard |

## 7. Revision History

| ***Date:*** | ***version #:*** | ***Description:*** | ***Updated by:*** |
|---|---|---|---|
| 02/28/2020 | 1.0 | Initial Draft | Security Team |
| 07/28/2023 | 1.1 | Verbiage and other pertinent updates | Julian Holman |
| 8/30/23 | 1.2 | Review and revisions | Chief Privacy Officer |