



# COLLIN COUNTY

Information Technology  
2300 Bloomdale Road  
Suite 3198  
McKinney, Texas 75071  
www.collincountytx.gov

|           |                                                |            |           |         |         |
|-----------|------------------------------------------------|------------|-----------|---------|---------|
| Policy #: | 020                                            | Effective: | 11/2/2015 | Page #: | 1 of 10 |
| Subject:  | Title: <b>Computer and Internet Use Policy</b> |            |           |         |         |

## 1.0 PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at Collin County. These rules are in place to protect the employee and Collin County. Inappropriate computer use exposes Collin County to risks including virus attacks, compromise of network systems, service interruptions and legal issues.

## 2.0 SCOPE

This policy applies to employees, contractors, consultants, temporaries, and other workers at Collin County including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Collin County.

## 3.0 REFERENCE

- Collin County Records Management Policy – March 2005
- 020A - Computer Systems and Internet Use Policy - User Acceptance Document
- 030 – Mobile Device Policy
- 003 – Desktop Password Policy

## 4.0 BACKGROUND

It is not the Information Technology Department's intention to impose restrictions contrary to Collin County's established culture of openness, trust and integrity. The Collin County Information Technology Department is committed to protecting the county, its employees and our partners from illegal or damaging actions by individuals.

Effective computer security is a team effort involving the participation and support of every Collin County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

The policy was created to give guidance to users on proper use of County equipment and networks.

## 5.0 POLICY

|             |     |             |             |       |           |
|-------------|-----|-------------|-------------|-------|-----------|
| Revision #: | 1.8 | Supersedes: | Version 1.7 | Date: | 11/2/2015 |
|-------------|-----|-------------|-------------|-------|-----------|



IT – Security Policy/Procedures

Last Updated and Saved: 10/15/2015 11:56:21 AM

|                  |                                                |                   |                  |                |                |
|------------------|------------------------------------------------|-------------------|------------------|----------------|----------------|
| <b>Policy #:</b> | <b>020</b>                                     | <b>Effective:</b> | <b>11/2/2015</b> | <b>Page #:</b> | <b>2 of 10</b> |
| <b>Subject:</b>  | <b>Title: Computer and Internet Use Policy</b> |                   |                  |                |                |

[General Policy](#)

[Password Policy](#)

[Internet and Intranet Use Policy](#)

[Social Media Use Policy](#)

[Personal Electronic Equipment Policy](#)

[Software License Policy](#)

[Third Party Non-Standard Software Policy](#)

[Donated and Grant Computer Equipment Policy](#)

[Express User Responsibilities](#)

## General Policy

It is the responsibility of the individual employee to read, understand, and abide by this and other policies in regards to the use of Collin County Information Technology systems.

While the Collin County Information Technology Department desires to provide a reasonable level of privacy, users should be aware that the data they create on Collin County systems remains the property of Collin County, is subject to Open Records Requests and possible legal procedures and as such use of Collin County systems constitutes a waiver of all rights to privacy. Due to the need to manage and protect the county's systems and network, Information Technology cannot guarantee the confidentiality of the information stored on any device used to access any county network. Additionally, all county data may be subject to Open Records Requests including any personal data that is stored on county systems. Use of personal mobile devices on a county network exposes that device to the same Open Records Requests.

For security and network maintenance purposes, authorized individuals within Collin County may monitor equipment, systems and network traffic at any time using either remote monitoring systems or manual data collection methods.

The use of Collin County automation systems including computers, fax machines, servers, networks, databases and all forms of Internet/Intranet access is for county business, by authorized personnel and for authorized purposes only. Brief and occasional personal use of county systems is allowed, as defined further in this policy document. Proper computer security habits and processes are the responsibility of each employee. Collin County employees are not to share user accounts, passwords or other user validation criteria with other employees or allow that information outside of the county. Computer passwords must be guarded and must not be written and posted on or near the computer or transmitted via the email system.

County computer equipment, files, user data, databases, programs or any other information on a County network represent County assets which can only be used for authorized County business. Use of County assets for personal gain or benefit is prohibited. Deleting, altering or sharing confidential, proprietary or other information

|                    |     |                    |             |              |           |
|--------------------|-----|--------------------|-------------|--------------|-----------|
| <b>Revision #:</b> | 1.8 | <b>Supersedes:</b> | Version 1.7 | <b>Date:</b> | 11/2/2015 |
|--------------------|-----|--------------------|-------------|--------------|-----------|

|                  |                                                |                   |                  |                |                |
|------------------|------------------------------------------------|-------------------|------------------|----------------|----------------|
| <b>Policy #:</b> | <b>020</b>                                     | <b>Effective:</b> | <b>11/2/2015</b> | <b>Page #:</b> | <b>3 of 10</b> |
| <b>Subject:</b>  | <b>Title: Computer and Internet Use Policy</b> |                   |                  |                |                |

upon termination of employment, either voluntary or involuntary, is prohibited and will be investigated and prosecuted to the fullest extent of the law.

County users are to store data in the official system of record. Personnel who are unsure of their system(s) of record are advised to contact their supervisor, department head or elected official for clarification on departmental policy. Collin County will maintain data stored on the county storage area network in departmental user data folders for a period of 6 (six) months with a rolling 30 day backup window. After the six month period, any data files belonging to inactive or terminated users may be subject to deletion from the storage system. Department heads and elected officials, as custodians of the records, are responsible for ensuring that the systems of record are used appropriately and contain the necessary data and comply with the county records retention policy. Systems outside of Collin County, like Dropbox or other external applications, are not part of the backup strategy.

Collin County maintains email records on the County Email Server for a period of 6 (six) months prior to deletion. It is the responsibility of the computer user, with guidance and training from the Records Management Officer and Information Technology staff, to manage e-mail messages and/or other electronic documents according to the county's retention policy and schedule. It is the responsibility of the sender of e-mail messages within the county's e-mail system and recipients of messages from outside the county to retain the messages for the approved retention period. Names of the sender, recipient, date/time of the message, as well as any attachments must be retained with the message.

Use of county computers, tablets, networks, and Internet access is a privilege and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- a. Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate county purposes;
- b. Engaging in unlawful or malicious activities; personal business activities; excessive use of instant messaging, chat rooms or other social media sites; usurping County business opportunities; soliciting money for personal gain; political campaign activity; or searching for jobs outside Collin County;
- c. Accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorization from someone with the right to make such a grant;
- d. Making unauthorized copies of county data;
- e. Destroying, deleting, erasing, or concealing county data, or otherwise making files or data unavailable or inaccessible to the county or to other authorized users of county systems;
- f. Violating the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way;
- g. Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the county's networks, systems, or those of any other individual or entity;

|                    |     |                    |             |              |           |
|--------------------|-----|--------------------|-------------|--------------|-----------|
| <b>Revision #:</b> | 1.8 | <b>Supersedes:</b> | Version 1.7 | <b>Date:</b> | 11/2/2015 |
|--------------------|-----|--------------------|-------------|--------------|-----------|

|                  |                                                |                   |                  |                |                |
|------------------|------------------------------------------------|-------------------|------------------|----------------|----------------|
| <b>Policy #:</b> | <b>020</b>                                     | <b>Effective:</b> | <b>11/2/2015</b> | <b>Page #:</b> | <b>4 of 10</b> |
| <b>Subject:</b>  | <b>Title: Computer and Internet Use Policy</b> |                   |                  |                |                |

- h. Using offensive or harassing statements or language in violation of federal EEO legislation in either public or private messages;
- i. Sending, receiving, soliciting or accessing pornographic materials, sexually oriented messages or images;
- j. Causing congestion, disruption, disablement, alteration, or impairment of county networks or systems;
- k. Failing to log off, lock or otherwise secure any secured controlled-access computer or other electronic data system to which you are assigned, if you leave such computer or system unattended;
- l. Defeating or attempting to defeat security restrictions on county systems and applications;
- m. Installing third party software, whether vendor supplied or personally owned, on county system without authorization from the Information Technology Department;
- n. Removing any Collin County computer systems from county premises unless authorized by the Collin County Chief Information Officer, the employee's Department Head or Elected Official and the proper paperwork is completed, ***with the exception of laptops or tablets issued to County employees expressly to provide mobility and ability to work outside normal operating hours.***
- o. Downloading and installing inappropriate software without the prior approval of Collin County's Information Technology Department;
- p. Dissemination or printing of copyrighted materials, including articles and software, in violation of copyright laws;
- q. Visiting sites featuring pornography, terrorism, espionage, theft or drugs;
- r. Gambling or engaging in any other activity in violation of local, state or federal law;
- s. Unethical activities or content, or activities or content that could damage Collin County's professional reputation;
- t. ***Exceptions to the above conditions will apply to the departments that require full access to the Internet for job related reasons. A request to gain access to other Internet sites must be provided by the Department Head or Elected Official to the County Chief Information Officer.***

Electronic communications should maintain the same standards of decorum, respect and professionalism used in the office environment.

## **Password Policy**

This policy covers passwords managed by Active Directory, Router Passwords, Local Account Passwords, and Voice System Passwords.

This policy also serves as a guideline for any applications which do not use Active Directory for authentication. Applications which maintain their own password routines will use this policy, in as much as it may apply, but modify the password to match the limitations of the application.

|                    |     |                    |             |              |           |
|--------------------|-----|--------------------|-------------|--------------|-----------|
| <b>Revision #:</b> | 1.8 | <b>Supersedes:</b> | Version 1.7 | <b>Date:</b> | 11/2/2015 |
|--------------------|-----|--------------------|-------------|--------------|-----------|

|                  |                                                |                   |                  |                |                |
|------------------|------------------------------------------------|-------------------|------------------|----------------|----------------|
| <b>Policy #:</b> | <b>020</b>                                     | <b>Effective:</b> | <b>11/2/2015</b> | <b>Page #:</b> | <b>5 of 10</b> |
| <b>Subject:</b>  | <b>Title: Computer and Internet Use Policy</b> |                   |                  |                |                |

Passwords must meet or exceed the following requirements:

- Where supported, passwords for any device, system and account must comply with:
  - Minimum of 10 characters in length:
    - At least 1 alpha character (A through Z in either Uppercase, lowercase or MixedCase)
    - At least 1 numeric character (0 through 9)
  - At least 1 special character (example: !, @, \$, ~, etc.)
- Passwords will expire every 60 days
- Passwords may not repeat more frequently than every 12 months
- Password entry will be locked after 10 failed attempts
- Password lockout will last for 10 minutes
- Workstation screen saver will be set to require password entry after 5 minutes

Passwords must be protected and are to be treated as secure and confidential information by County employees.

### **Internet and Intranet Use Policy**

The Internet is to be used to further Collin County's mission, to provide effective service of the highest quality to the county's citizens and staff and to support other direct job-related purposes. Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and career development. The various modes of Internet/Intranet access are county resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications.

Collin County systems are allowed to access the Internet only through county approved and secured Internet accounts. Employees are strictly accountable for the content of their Internet messages and activity. Individuals shall in no way attempt to circumvent filters and other security measures restricting access to files, data or networks.

Brief and occasional personal use of the electronic mail system or the Internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense or harm to the county or otherwise violate this policy. Limited personal use of Internet resources is a special exception to the general prohibition against the personal use of computer equipment and software.

Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication should not be used to solicit or sell products or services that are unrelated to county business or distract, intimidate, or harass coworkers or third parties or otherwise disrupt the workplace.

|                    |     |                    |             |              |           |
|--------------------|-----|--------------------|-------------|--------------|-----------|
| <b>Revision #:</b> | 1.8 | <b>Supersedes:</b> | Version 1.7 | <b>Date:</b> | 11/2/2015 |
|--------------------|-----|--------------------|-------------|--------------|-----------|

|                  |                                                |                   |                  |                |                |
|------------------|------------------------------------------------|-------------------|------------------|----------------|----------------|
| <b>Policy #:</b> | <b>020</b>                                     | <b>Effective:</b> | <b>11/2/2015</b> | <b>Page #:</b> | <b>6 of 10</b> |
| <b>Subject:</b>  | <b>Title: Computer and Internet Use Policy</b> |                   |                  |                |                |

To minimize vulnerabilities on county computer systems, all downloaded Internet files will be scanned with virus detection software before being opened or viewed. Employees may not attempt to bypass or circumvent the County anti-virus program.

The Collin County website is a useful tool that provides a means for departments to communicate and provide services to the citizens of our county. Departments have the opportunity to establish and maintain a department webpage within the county web site. Departments are responsible for ensuring that the content will be reviewed, approved and published to the production web site by the Information Technology Department and/or the County Public Information Officer.

### **Social Media Use Policy**

The County Public Information Officer has responsibility to act as the official County spokesperson which includes the county web presence and social media communications. Official county social media outlets will be maintained by the Public Information Officer with assistance from the Information Technology department.

As social media has gained a more prominent role within society the value of this medium as a work aid has become more apparent. Use of social media, as a job aid, is governed and bound by the General Policy and the Internet and Intranet Use Policy. Employee's use of social media sites in the performance of their job duties should be discussed with the employee's management so they may be kept informed of how that tool aids the delivery of county services. When using social media sites employees are not authorized to represent the County unless they have received direct authorization to do so by the County Public Information Officer.

Personal use of social media sites, while using county computer equipment, should be limited to brief and occasional use in accordance with the Internet and Intranet Use Policy. Messages posted to social media sites, using county computer equipment, may not contain inappropriate conduct or messages as specified in the General Policy.

While the county cannot dictate what employees, as private citizens, post on social media sites, the county does encourage employees to consider the potential impact their words, positions and postings may have as public servants and encourage all employees to act with decorum and restraint. Employees are cautioned that social media postings may sometimes take a life of their own and may persist in some form much longer than anticipated or desired.

### **Personal Electronic Equipment Policy**

Employees are not allowed to connect personal computer equipment to the Collin County Local Area Network (LAN) via a network cable and attempt to authenticate to the county network without express written consent of the County Chief Information Officer. As a

|                    |     |                    |             |              |           |
|--------------------|-----|--------------------|-------------|--------------|-----------|
| <b>Revision #:</b> | 1.8 | <b>Supersedes:</b> | Version 1.7 | <b>Date:</b> | 11/2/2015 |
|--------------------|-----|--------------------|-------------|--------------|-----------|

|                  |                                                |                   |                  |                |                |
|------------------|------------------------------------------------|-------------------|------------------|----------------|----------------|
| <b>Policy #:</b> | <b>020</b>                                     | <b>Effective:</b> | <b>11/2/2015</b> | <b>Page #:</b> | <b>7 of 10</b> |
| <b>Subject:</b>  | <b>Title: Computer and Internet Use Policy</b> |                   |                  |                |                |

convenience to county employees a secured wireless network, “wifiCCmobile”, is available as defined by policy document: 030 – Mobile Device Policy.

As identified in that policy, any connection settings on the user device, and installation of any client side applications, are the responsibility of the employee. Employees may be required to agree to an acceptable use statement, install remote data management software, accept software updates or patches and agree to allow Collin County to remotely remove data from any device which may be deemed to be compromised. By use of the “wifiCCmobile” network, county employees implicitly agree to the following conditions:

- Any personal data lost due to remote deletion is an acceptable risk and the employee will hold the county harmless should that event occur
- The IT department will not provide support or assistance for personal devices
- Personal devices used to connect to the wireless network may be subject to open records requests and potential seizure in the event of a law enforcement investigation
- Access to the wireless network is authenticated through the county’s Active Directory system which, along with other supporting network management tools, may be used to track user activity
- Network bandwidth is not guaranteed and capacity may be limited in order to allow other county networks to operate more efficiently during peak load times

Note to all County Personnel: Collin County in general (specifically the Information Technology Department and/or its employees) is not legally required to support, and cannot be held liable, for County personnel’s “personal” electronic devices. Personal devices include, but are not limited to desktops, laptops, tablets, iPods, cell phones, smart phones, video cameras, etc. Any assistance provided by an Information Technology staff member will be by the user’s request and a “Release of Liability Form” must be signed and returned to the Information Technology office where it will be kept on file. Upon signed receipt of this form and consent to proceed from the Information Technology Chief Information Officer and/or Assistant Director, a technician may be assigned to proceed with assistance *as County workload demands allow*.

If network connectivity has been approved and provided from your personal system to the Collin County network, you as a Collin County employee are directly responsible for securing your device and its content from outside sources. Securing your device should include password and virus protection on the device, as well as physically securing your device in public access areas. Please note, if your personal system is utilized, in part or in whole, for County business then it is subject to Open Records Requests just as any other computer device connected to the county network.

### Software License Policy

Collin County does not condone the illegal duplication of software or other copyrighted material. Per U.S. Copyright Law, illegal reproduction of software can be subject to civil

|                    |     |                    |             |              |           |
|--------------------|-----|--------------------|-------------|--------------|-----------|
| <b>Revision #:</b> | 1.8 | <b>Supersedes:</b> | Version 1.7 | <b>Date:</b> | 11/2/2015 |
|--------------------|-----|--------------------|-------------|--------------|-----------|

|                  |                                                |                   |                  |                |                |
|------------------|------------------------------------------------|-------------------|------------------|----------------|----------------|
| <b>Policy #:</b> | <b>020</b>                                     | <b>Effective:</b> | <b>11/2/2015</b> | <b>Page #:</b> | <b>8 of 10</b> |
| <b>Subject:</b>  | <b>Title: Computer and Internet Use Policy</b> |                   |                  |                |                |

damages of as much as \$100,000 per work copied and criminal penalties including fines and imprisonment. County employees who make, acquire, or use unauthorized copies of software will be subject to the above law.

Collin County purchases or licenses the use of computer software from a variety of outside companies. Collin County does not own the copyright to this software or its related documentation and unless authorized by the software developer does not have the right to reproduce it for use on more than one computer. With regard to the use on local area networks or on multiple machines, employees shall use software only in accordance with the license agreement. Information Technology personnel shall install all computer software unless the employee is specifically authorized to do so by the Information Technology department.

County software licenses shall not be used for personal use on non-county computer equipment.

Software license purchased by employees or received from vendors for personal use is prohibited on Collin County equipment.

The Collin County Information Technology Department is authorized to conduct random software license audits of its network and systems.

### **Third Party Non-Standard Software Policy**

Collin County provides a standard set of productivity software for the major lines of business operated by the county. The Information Technology department will either provide or assist with coordination of technical and functional support for this standard set of productivity applications. Since not all business needs may be met within this standard set of applications certain departments may be authorized to budget for, and procure, Third Party Non-Standard Software to accomplish specific business needs.

As implied by the name, Third Party Non-Standard Software is not part of the standard productivity suite and, as such, the Information Technology department does not have expertise with these software tools. While the Information Technology department will make every effort to assist with these applications the business users will ultimately be responsible for being self-sufficient and self-supporting.

Information Technology personnel must install the software on county owned assets and move the software between computers as needed. Periodic software updates and enhancements must be coordinated with the Information Technology Service Desk.

### **Donated and Grant Computer Equipment Policy**

Donated and grant supplied computer equipment may be incorporated into the county's technical infrastructure provided that the equipment has followed the proper Collin

|                    |     |                    |             |              |           |
|--------------------|-----|--------------------|-------------|--------------|-----------|
| <b>Revision #:</b> | 1.8 | <b>Supersedes:</b> | Version 1.7 | <b>Date:</b> | 11/2/2015 |
|--------------------|-----|--------------------|-------------|--------------|-----------|

|                  |                                                |                   |                  |                |                |
|------------------|------------------------------------------------|-------------------|------------------|----------------|----------------|
| <b>Policy #:</b> | <b>020</b>                                     | <b>Effective:</b> | <b>11/2/2015</b> | <b>Page #:</b> | <b>9 of 10</b> |
| <b>Subject:</b>  | <b>Title: Computer and Internet Use Policy</b> |                   |                  |                |                |

County Commissioner's Court acceptance process as defined in the capitalization and/or grant policies. The Information Technology department will work with the departments to install and configure properly accepted equipment on the county network.

Collin County will only provide standard software licenses for the systems provided by the county. Donated and/or grant equipment may require additional software licenses in order to connect to county networks, servers and storage disks or to utilize standard business productivity software. The Information Technology department does not have additional budget dollars available to provide for these licenses. Departments are encouraged to work with the Information Technology department to identify any required software licenses so that the department may request the appropriate funds at the time the equipment is accepted by Commissioner's Court. Failure of the department to obtain the required software licenses may result in the equipment not being installed on the county network.

### **Express User Responsibilities**

Computer users are responsible for the appropriate use of county computers and for taking reasonable precautions to secure the information and equipment entrusted to them. Employees are responsible for reporting inappropriate use of county computers and breaches of computer security and assisting in resolving such matters.

Any employee who learns of a violation of this policy should notify the appropriate Collin County elected official, department head, or the Information Technology Department.

## **6.0 PROCEDURES**

N/A

## **7.0 REVISION HISTORY**

| <b>Date</b> | <b>Revision #</b> | <b>Description of Change</b>                                                                                              |
|-------------|-------------------|---------------------------------------------------------------------------------------------------------------------------|
| 11/11/2003  | 1.0               | Initial creation - CDivers                                                                                                |
| 06/01/2004  | 1.1               | Revised - CDivers                                                                                                         |
| 05/26/2005  | 1.2               | Revised – Dan Kennedy                                                                                                     |
| 09/01/2010  | 1.3               | Revised – Security Team                                                                                                   |
| 12/28/2010  | 1.4               | Revised – CDivers – Added “Release of Reliability” statement for all personal equipment. Added I Pad’s to equipment list. |
| 1/10/2013   | 1.5               | GElliott – Rewrite of general policy, insertion/alignment with other policy positions                                     |

|                    |     |                    |             |              |           |
|--------------------|-----|--------------------|-------------|--------------|-----------|
| <b>Revision #:</b> | 1.8 | <b>Supersedes:</b> | Version 1.7 | <b>Date:</b> | 11/2/2015 |
|--------------------|-----|--------------------|-------------|--------------|-----------|

|                  |                                                |                   |                  |                |                 |
|------------------|------------------------------------------------|-------------------|------------------|----------------|-----------------|
| <b>Policy #:</b> | <b>020</b>                                     | <b>Effective:</b> | <b>11/2/2015</b> | <b>Page #:</b> | <b>10 of 10</b> |
| <b>Subject:</b>  | <b>Title: Computer and Internet Use Policy</b> |                   |                  |                |                 |

|           |     |                                                                                                                            |
|-----------|-----|----------------------------------------------------------------------------------------------------------------------------|
| 4/21/2014 | 1.6 | GElliott – Inclusion of new password policy; Policy Document 003 - Desktop Password Policy                                 |
| 12/3/2014 | 1.7 | GElliott – Added clause about network data retention and EO/DH responsibility to ensure data saved in the system of record |
| 11/2/2015 | 1.8 | GElliott – Added clause for privacy waiver                                                                                 |

## 8.0 INQUIRIES

N/A

## 9.0 APPENDICES

N/A

|                    |     |                    |             |              |           |
|--------------------|-----|--------------------|-------------|--------------|-----------|
| <b>Revision #:</b> | 1.8 | <b>Supersedes:</b> | Version 1.7 | <b>Date:</b> | 11/2/2015 |
|--------------------|-----|--------------------|-------------|--------------|-----------|