

THE STATE OF TEXAS

COUNTY OF COLLIN

POLICY
AMEND
COLLIN COUNTY COMPUTER OPERATING
& SECURITY POLICY
INFORMATION TECHNOLOGY

On June 7, 2005, the Commissioners Court of Collin County, Texas, met in regular session with the following members present and participating, to wit:

Ron Harris
Phyllis Cole
Jerry Hoagland
Joe Jaynes
Jack Hatchell

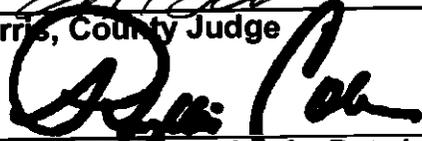
County Judge, Presiding
Commissioner, Precinct 1
Commissioner, Precinct 2
Commissioner, Precinct 3
Commissioner, Precinct 4

During such session the court considered a request for approval to amend the Collin County Computer Operating & Security Policy.

Thereupon, a motion was made, seconded and carried with a majority vote of the court for approval to amend the Collin County Computer Operating & Security Policy. Same is hereby approved in accordance with the attached documentation.



Ron Harris, County Judge



Phyllis Cole, Commissioner, Pct. 1



Jerry Hoagland, Commissioner, Pct. 2



Joe Jaynes, Commissioner, Pct. 3



Jack Hatchell, Commissioner, Pct. 4

ATTEST:



Brenda Taylor, Ex Officio Clerk
Commissioners' Court
Collin County, TEXAS





Information Services

To: Judge Ron Harris
210 S. McDonald
McKinney, TX, 75069

From: Dan Kennedy, Assistant IT Director
Cc: Caren Skipworth, IT Director
Date: May 31, 2005
Subject: Policy Update – Collin County Computer Operating & Security
Policy Manual, v.1.3

The Information Technology department is requesting a change to the current Collin County Computer Operating & Security Policy Manual, v1.3. The changes address data disposal, file recovery, instant messaging, and email.

Additions to policy are underlined; deletions are italicized.

Administrative Matters – Disposal of Data

Existing text to be deleted:

Disposal of County Data

Purge files that no longer have a practical use on a periodic basis. Old computer files utilize disk space, and often represent a potential hazard to you and the County. Typically, dated information is only useful to individuals who should not have the data. It is recommended that files (data) that is 2 years or older be archived and deleted from the main system.

A word of caution, permanently removing a file from your computer is something you need to consider carefully before taking action. Recreating a file you did not intend to delete is tedious and time consuming. Although the file probably exists on backup, it is not always practical for the Information Technology department to expend the resources necessary to find the file. The LAN backup is principally designed to recover the entire system, not a single file.

Recommended text:

Disposal of County Data

All employees are required to follow Collin County's Records Management policies and procedures when considering removing any files that no longer have a practical use on a regular basis. While old computer files utilize disk space, often represent a potential hazard, and are subject to the Public Information Act, employees are required to assess whether the files are County records or not. If so, adopted retention requirements must be applied to the record (file). LAN backups are not designed to serve as an individual file retrieval tool, but are intended to recover the entire system.

It is recommended that county employees review files that have not been accessed in at least two years and if these files are not County records that, the files be deleted or archived. Remember that if these files are retained, they are subject to the Texas Public Information Act.

Elected officials/department heads are responsible for ensuring that their employees understand Collin County's computer and records policies and apply them to all County records including e-mail.

Administrative matters - File Recovery section as follows:

Existing text:

Computer files and e-mail are rarely erased from the system simply by hitting the delete key. Rather, they are stored in a random place on the computer. These files can be easily recovered by running a file recovery program. To actually erase a deleted file from existence, you must run a program to erase deleted files. Keep in mind that if the files are backed-up before you run the program, you again have an electronic record. Files stored on the LAN are much more difficult to erase. This is because the LAN is backed up automatically, and only the Information Technology department has access to run programs that will permanently erase a file from the server. The bottom line is, your deleted file is most likely permanently stored on backup.

Recommended text:

Computer files and e-mail are rarely erased from the system simply by hitting the delete key. Rather, they are stored in a random place on the computer. These files can be easily recovered by running a file recovery program. Current computer forensics technology allows the recovery of data erased from magnetic storage media and written over many times. To actually erase a deleted file from existence, you must run a program to erase deleted files. Keep in mind that if the files are backed-up before you run the program, you again have an electronic record. Files stored on the LAN are much more difficult to erase. This is because the LAN is backed up automatically, and only the Information Technology department has access to run programs that will permanently erase a file from the server. The bottom line is, your deleted file is most likely permanently stored on backup for a short period.

Recreating a file you did not intend to delete is tedious and time consuming. Although the file probably exists on backup, it is not always practical for the Information Technology department to expend the resources necessary to find the file. The LAN backup is principally designed to recover the entire system, not a single file.

External Communications – add section under instant messaging.

The use of instant messaging communications is not approved for use in conducting County business. If a legitimate, business need exists for access to this technology, the employee's Elected Official/Department Head must make a request in writing to the Director of Information Technology justifying this access. The Director of Information Technology will determine if access is granted.

E-mail – add the following text after third paragraph that ends "...standard names are assigned by the Information Technology department."

Personal use of e-mail is a privilege, not a right. Abuse of the privilege may result in appropriate disciplinary action. The content and function of an e-mail message determines if the e-mail is a local government record as well as its retention period. Recorded e-mail messages that fall under the definition of local government records are the property of Collin County and therefore the taxpayers of the county. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to local government records retention.

Elected Officials/Department heads are responsible for ensuring that their employees follow this policy.

Glossary – add terms

County (local Government) Record – any document, paper, letter, book, map, photography, sound or video recording, microfilm, magnetic tape, electronic medium or other information recording medium, regardless of physical form or characteristic and regardless of whether public access to it is open or restricted under laws of the state, created or received by a local government or any of its officers or employees pursuant to law, including an ordinance, or in the transaction of public business. (Local Government Code §201.003(8)) The term does not include (a) extra identical copies of documents created only for convenience of reference or research, (b) notes, journals, diaries, and similar documents created by an officer or employee of the local government for the officer's or employee's personal convenience, (c) blank forms, (d) stocks of publications, (e) library and museum materials acquired solely for the purpose of reference or display, (f) copies of documents in any media furnished to members of the public to which they are entitled under Chapter 552, Government Code or other state law, and (g) any records, correspondence, notes, memoranda, or documents other than a final written agreement described by Section 2009.054(c), Government Code

Electronic media – all media capable of being read by a computer including computer hard disks, magnetic tapes, optical disks, or similar machine-readable media.

Electronic Record – the information that is maintained in electronic format in a computer for computer processing and the product of computer processing of that information that satisfies the definition of “local government record data” in the Local Government Code §205.001.

Local government record data – the information that by law, regulation, rule of court, ordination, or administrative procedure in a local government comprises a local government record as defined by Local Government Code, §205.003.

Transitory Information – records of temporary usefulness that are not an integral part of a records series, that are not regularly filed within a recordkeeping system, and required only for a limited period of time for the completion of an action by an employee or official; not essential to fulfillment of statutory obligations or document departmental functions.

**COLLIN COUNTY INFORMATION
TECHNOLOGY Computer Operating &
Security Policy Manual Version 1.4
2005**

Table of Contents

Purpose.....	3
Introduction.....	4
Computer Users.....	5
Unauthorized Access.....	5
Computer Sabotage	5
Password Selection and Protection	5
Password Cracking.....	6
Easy to Remember and Hard to Crack.....	6
Password Access Program	6
Snooping	7
Hackers	7
Viruses, Worms and Trojan horses.....	7
Confidentiality	8
General.....	8
Handling Confidential Information	8
Encryption	9
Physical Security.....	9
Locks.....	9
Laptops.....	9
Off-Site Computers	10
Administrative Matters.....	10
Back-up	10
Copyright Infringement.....	10
Harassment, Threats and Discrimination	11
Accidents, Mistakes and Spills.....	12
Unauthorized Changes to County Computers.....	12

Purchases of Computer Software and Equipment.....	12
Disposal of County Data	13
File Recovery.....	13
Personal Use of Computers	14
Proprietary Information.....	14
Reporting Policy Violations.....	14
Termination of Employment	15
Privacy	15
Monitoring Computer Communications and Systems	15
Lawsuits and Subpoenas.....	16
External Communications	16
Third Parties	16
Dangers of the Internet	17
Internet Connections	17
Filtering Services.....	17
Business Reputations.....	18
Remote Access	18
E-mail	18
Electronic Communications.....	19
Forwarding Information	20
Spam.....	20
Intranet.....	21
WEB Site	21
Local Area Network	22
Glossary of Terms.....	22

Operating and Security Policy Manual

Purpose

The purpose of the Computer Operating and Security Policy Manual is to provide Collin County Elected Officials and Department Heads information to help protect the County and employees of the County from liability and business interruptions due to inappropriate use of computers and breaches of computer security.

Elected Officials/Department Heads and Managers are responsible for ensuring that their employees follow this policy.

This policy documents the computer users' responsibility to safeguard computer equipment and information from accidental or deliberate unauthorized access, tampering, snooping, distribution, or destruction. It sets forth what is, and is not, appropriate use of Collin County computers. Users may be disciplined for noncompliance with County policy. This policy does not purport to address every computer operating and security issue. It is your responsibility to use sound judgment. Should you identify an issue or situation that you are not certain how to deal with, inquire of management.

The Employee Computer Operating and Security Policy is subordinate to any collective bargaining agreement, employment contract, or other employment agreements. The County may add to, or change, the policies at any time.

Introduction

In the early days when computers were centralized and managed by data centers, using the computer was very different. Computers were housed in cold rooms with big padlocks and only computer technicians, and other authorized personnel had access. Links to the outside world were unusual, and the purpose of the computer was principally for computing. In addition, and more importantly, while some very important systems were maintained on these computers, they represented only a few systems such as accounting, payroll, billing, and the like. Computers did not house every single aspect of our work life, from our most important, confidential documents and worksheets, to our daily communications and calendar.

Portable and desktop computers have changed all that. Today, many people have access to computers. With the continuing increase in the power of computers, and the number of employees using computers, the time spent on computers can only increase. Because so much important work is stored on computers, and computers are used for maintenance and transmission of County records, it is important that management provide guidance on proper use of County computers and computer services.

The impact of the computer on our government business has been significant, and at breakneck speed. The technology accessible today could not have been speculated just five or ten years ago. Who knows what we will have available to us in a few more years. Keeping technology current is key to our competitiveness, and provides unprecedented opportunity for Collin County and its employees to succeed. In that same vein, it puts us at considerable risk. Implementing new technologies is expensive, time consuming, and without established policies and practices in place, could lead to disaster. We do not have to look very far to find numerous examples of private or public entities that have incurred substantial losses due, in part, to the computer. **The first, best, and most important line of defense starts with our employees!**

It is unquestioned that a well-trained work force properly versed in computer operating procedures, and computer user security matters, will have the best chance of minimizing business interruptions due to inappropriate, negligent, or unethical use of County computers. For this reason, we have created the Employee Computer Operating and Security Policy. Please understand it is not our intention to encumber your use of the computer, but rather our fiduciary responsibility to protect the resources of the County. We believe this policy accomplishes that with little to no hardship to you, the computer user and our valued employee.

Computer Operating and Security Policy Manual

Computer Users

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. Users are responsible for adhering to County policies and practices as described herein, and in other County policy manuals, to ensure County computers are used in accordance with County policy guidelines, and reasonable measures are taken to prevent loss or damage of computer information and equipment.

Unauthorized Access

Unauthorized access of County computers is prohibited. Unauthorized access of third-party computers, using County computers, is prohibited. Attempting to access County computers without specific authorization is prohibited. Any form of tampering, including snooping and hacking, to gain access to computers is a violation of County policy, and carries serious consequences. Employees are required to signoff (logoff) all computer systems at the end of the day, and when not in use for an extended period of time. This will help prevent computer security breaches, and protect your system. In addition, computer users must take other reasonable precautions to prevent unauthorized access of County computers.

Computer Sabotage

Destruction, theft, alteration, or any other form of sabotage of County computers, programs, files, or data is prohibited and will be investigated and prosecuted to the fullest extent of the law.

Password Selection and Protection

Select difficult passwords. Change them regularly, and protect them from snoopers. A lot of damage can be done if someone gets your password. Users will be held accountable for password selection and protection.

Do not share your password with anyone, other than a designated County

official. Do not write it down where someone can find it, do not send it over the Internet, Intranet, e-mail, dial-up modem, or any other communication line. Poor password selection and safekeeping is not comforting to management investigating a computer security breach, nor is it an acceptable excuse if a hacker damages County computer systems using your password.

Password Cracking

It is not uncommon for employees to try to figure out a friend's, or associates, password, just to see if they can. However, the same employee would never steal the key and go through your desk drawer, looking at everything and anything private and confidential. Yet, this is just what happens when passwords are cracked. Stay away from such activity. It is a serious violation of County policy.

Easy to Remember and Hard to Crack

Another concern is forgetting your password. Getting into your computer when you have forgotten the password is, in some cases, very difficult. A good method to help you remember your password is to select passwords that are unique to you, and try to use it at least once every day. For example, if you live on Elm Street, do not select "elm" as a password. Select the nearest crossroad and always finish, or start, with a number (maybe your favorite number).

The following is a good guideline for password selection:

- ◆ Use 6 or more characters, and at least one alphanumeric character (Combination of any characters can be used – try to avoid words that can be found in the dictionary)
- ◆ Your password should not include your login (Profile) name, your name, your spouse's or partner's name, children's or pet's name, or any other names commonly known to others
- ◆ Your password should not be a word pertaining to the County, your work, or an activity that you participate in or follow that is commonly known
- ◆ Your password should not include anything derogatory, offensive, or defamatory
- ◆ You will be required to change your password every 90 days.
- ◆ You can't reuse an old password over and over again. If you have a question about password selection or safekeeping, please contact the Information Technology Department.

Password Access Program

The County's password access program is an excellent tool to defend against

unauthorized access of County computers. However, a password access program is only effective when used properly. Do not leave your computer logged on and unattended for an extended period of time. Do not log on to your system if someone can see you keying in your password (there is no need to create the temptation). Make sure the password access program is set to deny access to your computer after three unsuccessful attempts (this makes it difficult for someone using a program designed to crack passwords to successfully access your computer). Report any irregularities flagged by the password access program (last login time and date, number of attempts to login, etc.). At night when you leave, Logoff (signoff) your computer. If you use a remote access program, and you need to leave your computer on, be sure that it is in a locked room.

Snooping

Snooping into County computer systems is a serious violation of County policy. If you have no business being there, don't go there. If you accidentally identify a new way to access information, report it to the Information Technology Department. Watching other users enter information, and looking at computer disks that do not belong to you, are prohibited. Obtaining, or trying to obtain, other users' passwords, or using programs that compromise security in any way, are violations of County policy. If you observe someone snooping, report it to the Elected Official/Department Head or the Information Technology department.

Hackers

Never give any information about computer systems out over the telephone, or in any other way. If someone requests such information, get their name and phone number, and tell them you will get right back to them. Report the incident immediately to the Elected Official/Department Head or the Information Technology department. Without your help, the County has little chance of protecting the County's computer systems.

Using hacker programs and trying to access computer systems using hacker techniques is prohibited. Trying to hack into third party computer systems using County computers is prohibited, and will be reported to the local authorities. Hacker crimes result in millions of dollars of downtime, lost data, and other problems. If you are caught hacking, it is a serious offense. If you identify vulnerability in the County's computer security system, report it to the Elected Official/Department Head or the Information Technology department.

Viruses, Worms and Trojan horses

It is critical that users make certain that data and software installed on County computers are free of viruses. Data and software that have been exposed to any computer, other than County computers, must be scanned before installation. This includes e-mail with attachments (a virus can quickly contaminate your computer simply by opening an e-mail attachment), downloads from the Internet and other sources of data that may be contaminated. Viruses can result in significant damage, and lost productivity. If you are uncertain whether data or software needs to be scanned before installation, contact the Information Technology department.

Use of virus, worm, or trojan horse programs is prohibited. If you identify a virus, worm, or trojan horse, or what you suspect to be one, do not try to fix the problem. Immediately turn your computer off, make notes as to what you observed, and contact the Information Technology department. The principal concern is stopping the contamination before additional damage is done. These programs are most successful when ignored. They are designed to easily hop from application to application, contaminate a computer disk, and access another computer. They easily travel down phone, cable, ISDN, or other communication lines, infect e-mail, data and files, and find their way to other computer systems. The key to containment is limiting the reach of the contamination. Turning off your computer does this best.

Confidentiality

General

All computer information is considered confidential unless you have received permission to use it. Accessing or attempting to access confidential data is strictly prohibited. Confidential information should only be used for its intended purpose. Using confidential information for anything other than its intended use is prohibited, without prior management approval.

Handling Confidential Information

Confidential information stored on computers is typically more difficult to manage than traditional paper documents that are sealed in an envelope, and locked in a filing cabinet clearly labeled CONFIDENTIAL. As such, it is important that users take extra care with confidential information stored on computers. The following are inappropriate under normal circumstances when dealing with confidential information:

- ◆ Printing to a printer in an unsecured area where documents may be read by others
- ◆ Leaving your computer unattended with confidential files logged on to

your system ♦ Making unauthorized copies of confidential data ♦ Leaving computer disks with confidential data unattended, in easy to access places.

Remember it only takes a minute to copy a disk ♦ Sending confidential information over the Internet, Intranet, dial-up modem lines, or other unsecured communication lines without approval from the Elected Official/Department Head or the Information Technology department If you observe a document at a shared printer, or any other location, do not read it without permission.

Encryption

Encryption and encryption utilities are prohibited without Elected Official/Department Head or the Information Technology department. If you need to send confidential or proprietary information over the Internet, or other public communication lines, you must obtain prior approval.

Physical Security

Locks

Physical security is key to protecting your computer and computer information from loss and damage. Store floppy disks and other sensitive information in a locked drawer. You are required to logoff (signoff) your computer when it is not in use for an extended period of time. Lock the door to your office, if you have one. Take a few minutes to practice good physical security. Your investment of time will provide an excellent return, and help prevent temptation by others.

Laptops

There is no sure way to secure laptops. However, there are many sensible, cost-effective measures that can help reduce the risk of loss or damage. The following are required when taking laptops off County property:

- ♦ Report lost or stolen computers immediately to the Information Technology department. ♦ All important files must be backed-up, and back-up disks must be stored in a separate physical location from the computer ♦ Confidential, important, and proprietary data leaving the facility requires authorization ♦ Use reasonable

precautions to safeguard the laptop against accidental damage. ♦ When traveling, laptops must be in sight at all times or physically secure
♦ Always store laptops in a concealing carrying case

Off-Site Computers

Off-site users must take additional precautions to safeguard computer information and equipment, including but not limited to:

♦ Safeguarding the computer and information from theft or damage ♦ Prohibiting access to the computer (including family, friends, associates, and others) for any purpose, without authorization ♦ Adhering to all computer policies and practices of the County for on-site users

Administrative Matters

Back-up

Users are responsible for regular back up of essential computer files, and secure storage of back-up disks. It takes about four hours to replace a computer. With proper back-up practices, it should take about the same amount of time to replace the data.

All backed-up files should be stored on a secure computer disk or tape, other than the one containing the original data. The back-up disk or tape should be stored on site, preferably in a locked drawer.

All important, confidential, or proprietary information must be stored on the local area network (LAN). The LAN is equipped with electronic and physical security. Activity on the network is monitored for tampering, and other security breaches. Maintenance and back up are performed on the LAN daily. Programs and other information are updated on the LAN regularly. Use the LAN; it is safe, effective, and reliable.

Copyright Infringement

The County does not own computer software, but rather licenses the right to use software. Accordingly, authorized County officials in accordance with the terms of the software licensing agreements may only reproduce County licensed software.

Unauthorized copying, redistributing, and republishing of copyrighted or proprietary material are strictly prohibited. Copyright laws apply on the Internet as well. There is no "but copying it was so easy" defense to copyright infringement. Copyright infringement is serious business, and the County strictly prohibits any such activity. If you have questions about copyright infringement, discuss it with management immediately.

Copies of shareware or "free" programs must be registered with the Information Technology department. Shareware and free software often have licensing and use restrictions, and should not be copied or forwarded to others. Typically, if you continue to use shareware you must send in a "donation," often of a specified amount. If you neglect to do so, you may have committed copyright infringement. If you provide the program to a friend, you may have violated copyright law. It is not unusual for "free" software to contain a virus. As such, it is important that all new software is registered with the Information Technology department. Your supervisor and the Information Technology department must approve requests for application programs. All software on County systems must be approved and installed by the Information Technology department.

Harassment, Threats and Discrimination

It is County policy, and the law, that employees are able to work free of unlawful harassment, threats, and discrimination. Unlawful harassment is physical or verbal behavior directed towards an individual due to their race, age, marital status, gender, disability, religion, sexual orientation, or nationality for the purpose of interfering with an individual's work performance, or creating an intimidating or hostile work environment.

It is not uncommon for employees to receive files, data, pictures, games, jokes, etc., that may be considered offensive by some. Currently, there are many cases in the courts addressing just such issues, the ramifications of which are significant. The computer is possibly the easiest tool for obtaining, storing, sharing, and disseminating to large audiences such material and viewpoints. Stay away from such activity; it is a serious violation of County policy. It is inappropriate to use County computers to share your personal views about religion, politics, sexuality, or any other subject of a personal nature that could be considered offensive to others within or outside the County. County computers are not vehicles to express free speech. Do this on your own time, away from the County, using your own resources.

Computers provide a huge potential for unlawful harassment. Users often think their communications are private, and trashed or deleted files are gone forever. However, deleted files are often easily recovered; and information on County computers is not necessarily private. Users often feel comfortable writing and storing files within the confines of their "personal" computer, and sharing

personal views on a wide range of non-business subjects. Remember, whatever you transmit is a permanent record to the receiver. It can, at some future date, be taken out of context and used against you and the County.

The County provides (purchases) the computer equipment and services and therefore has ownership of all electronic files. These files include e-mail, data, images. (etc)

Accidents, Mistakes and Spills

It is not hackers, snoopers, viruses, worms, or trojan horses that cause the most damage to computers and information. It is, by far and away, us, the computer users. According to current research, authorized users do most data loss and damage to computers. Mistakes and accidents represent the biggest cost when it comes to computer information loss. We have all done it, deleted a file that we just spent hours creating, spilled coffee on the keyboard, or dropped the laptop on the floor.

"An ounce of prevention is worth a pound of cure" is a very appropriate cliché for computer operations. Take a few seconds to read the computer screen before you delete, save, or transmit files. In addition, users need to take reasonable precautions with respect to computer operations, maintenance, handling, and transportation. It is not our intention to prohibit coffee at your desk. However, when placing liquids, and other food items on your desk, please be careful.

Unauthorized Changes to County Computers

Installing software and making changes to computer hardware, software, system configuration, and the like are prohibited, without authorization. The County's computer systems have been designed and documented to prevent loss of data, and provide an audit trail for correcting problems. Unauthorized changes to computer systems ultimately result in lost productivity. Such changes often require a computer technician to fix both the original problem, and the problem caused by the would-be computer technician. Poor documentation of the procedures performed, and the order in which they were completed further complicate unauthorized changes to computer systems.

Purchases of Computer Software and Equipment

Purchases of computer software and equipment are prohibited without approval from the Information Technology department. All computer software and hardware purchases must be registered with the Information Technology department, meet pre-established quality requirements, be compatible with other

County computer software/hardware, and meet standard communications.

Disposal of County Data

All employees are required to follow Collin County's Records Management policies and procedures when considering removing any files that no longer have a practical use on a regular basis. While old computer files utilize disk space, often represent a potential hazard, and are subject to the Public Information Act, employees are required to assess whether the files are County records or not. If so, adopted retention requirements must be applied to the record (file). LAN backups are not designed to serve as an individual file retrieval tool, but are intended to recover the entire system.

It is recommended that county employees review files that have not been accessed in at least two years and if these files are not County records that the files be deleted or archived. Remember that if these files are retained, they are subject to the Texas Public Information Act.

Elected officials/department heads are responsible for ensuring that their employees understand Collin County's computer and records policies and apply them to all County records including e-mail.

File Recovery

Computer files and e-mail are rarely erased from the system simply by hitting the delete key. Rather, they are stored in a random place on the computer. These files can be easily recovered by running a file recovery program. Current computer forensics technology allows the recovery of data erased from magnetic storage media and written over many times. To actually erase a deleted file from existence, you must run a program to erase deleted files. Keep in mind that if the files are backed-up before you run the program, you again have an electronic record. Files stored on the LAN are much more difficult to erase. This is because the LAN is backed up automatically, and only the Information Technology department has access to run programs that will permanently erase a file from the server. The bottom line, your deleted file is most likely permanently stored on backup for a short period.

Recreating a file you did not intend to delete is tedious and time consuming. Although the file probably exists on backup, it is not always practical for the Information Technology department to expend the resources necessary to find the file. The LAN backup is principally designed to recover the entire system, not

a single file.

Personal Use of Computers

Incidental and occasional personal use of County computers is permitted for reasonable activities. As a general rule, if you would be uncomfortable asking for permission, it is probably not an appropriate use of County computers. Prohibited activities include, but are not limited to, computer games, personal software and hardware, writing your autobiography, and running a personal business on the side. Using County computers to store or transmit inappropriate jokes, junk mail, chain letters, or to solicit for commercial, religious, charitable, or political causes is prohibited. If you are uncertain about a specific activity, ask your supervisor. Personal files, information, and use of County computers will be treated no differently by the County than business use, with regard to employee privacy.

Many software games are illegally copied, and often contain viruses. Such programs represent a potential liability to you and the County. Proof of ownership and the authorization for use is required for all software on County computers by the Information Technology department. Coming to work with a computer game, on an unlabeled disk, you received from a friend of a friend, who obtained it at a "Hacker's Rule" convention, that may be contaminated with a virus that could corrupt other County computers, is prohibited. Proceeding to play the game on County time is irresponsible. We do not think in these terms when using computer games. However, it's time we start.

Proprietary Information

County data, databases, programs, and other proprietary information represent County assets and can only be used for authorized County business. Use of County assets for personal gain or benefit is prohibited. Sharing County proprietary information with County personnel, or third parties, is prohibited.

Reporting Policy Violations

Employees are required to report violations, or suspected violations, of computer policy. Activities that should immediately be reported to the Elected Official/Department Head or the Information Technology department include, but are not limited to:

- ◆ Attempts to circumvent established computer security systems
- ◆ Use, or suspected use, of virus, trojan horse, or hacker programs
- ◆ Obtaining, or trying to obtain, another user's password
- ◆ Using the computer to make harassing or defamatory comments, or to in any way create a hostile work environment
- ◆ Using the computer to communicate inappropriate messages or jokes that may

be considered offensive by others ♦ Illegal activity of any kind ♦ Trying to damage the County, or an employee of the County, in any way Computer policy violations will be investigated. Noncompliance with the County's employee computer policy may result in discipline up to, and including, termination. Employees that report violations, or suspected violations of County policy will be protected from termination, discrimination, harassment, and any other form of retaliation. Hackers, snoopers, password stealers, virus installers, data erasers, and anyone involved in such activity will be disciplined. If you identify computer security vulnerability, you are required to report it immediately.

Termination of Employment

All information on user computers is considered County property. Deleting, altering, or sharing confidential, proprietary, or any other information upon termination is prohibited. The computer you have been entrusted with must be returned with your password, identification code, and any other appropriate information necessary for the County to continue using the computer, and information, uninterrupted.

The following activity is prohibited upon termination, and will be prosecuted to the fullest extent of the law:

♦ Accessing County computers ♦ Providing third parties, or anyone else, access to County computers ♦ Taking computer files, data, programs, or computer equipment

Privacy

Monitoring Computer Communications and Systems

Many people think data stored on computers, transmission of data between individuals on dial-up modem lines, communications on the Internet, and e-mail are private, and in most cases they are. **However, the County reserves the right, without prior notice, to access, disclose, use, or remove both business and personal computer communications and information, and will do so for legitimate business purposes.**

Random audits to verify that County computers are clear of viruses, and used in accordance with County policy, may be performed. The County will investigate complaints about inappropriate images on computers, inappropriate e-mail, or other inappropriate conduct. The County may monitor Internet activity to see what sites are frequented, duration of time spent, files downloaded, and information exchanged.

Again, computer systems and information are County property, and should be used principally for business purposes.

Lawsuits and Subpoenas

County computers, like any other County property, are subject to subpoenas. This means that prosecutors and plaintiffs' attorneys may access County computers, and look at information to gather evidence in a complaint. It is not difficult to imagine how easy it would be to find embarrassing and possibly incriminating information on County computers. For attorneys skilled in electronic discovery, the wealth of information is immense.

It is not the Information Technology department intention to suggest that you remove any information from your computer, now or at any other time, to in any way hinder an investigation of any kind. Quite the contrary, the County prohibits such activity. The County's intention is to ensure that users conduct their work to the highest ethical and moral standards with the knowledge that computer information (even deleted files) can be used against you and the County in a legal proceeding.

External Communications

Third Parties

The same standards of decorum, respect, and professionalism that guide us in the office environment, apply to computer communications with third parties. Important, confidential, and proprietary information is stored on County computer systems. Accordingly, only County personnel are allowed access to the County's computer systems, without written authorization. The County must approve computer data and other information received by, or provided to, third parties. Please keep in mind that third parties may have a legitimate business need, duty, legal right, or obligation to access, disclose, or use information transmitted.

The use of instant messaging communications is not approved for use in conducting County business. If a legitimate, business need exists for access to this technology, the employee's Elected Official/Department Head must make a request in writing to the Director of Information Technology justifying this access. The Director of Information Technology will determine if access is granted.

Dangers of the Internet

Copyright laws can be enforced on the Internet. Viruses can be downloaded from the Internet. Inappropriate web sites, images, and communications exist on the Internet. Competitors exist on the Internet. Hackers exist on the Internet. As such, users must follow established computer operating policies and practices to reduce the opportunity for security breaches, and inappropriate or illegal activity resulting from connecting to the Internet.

Internet Connections

Internet connections are authorized for specific County business needs only. Connection to the Internet without the authorization by the Elected Official/Department Head or the Information Technology department is prohibited. Furthermore, the following activities are prohibited without authorization:

- ◆ Accessing the Internet without an approved firewall
- ◆ Downloading information of any kind, including data, files, programs, pictures, screen savers, and attachments
- ◆ Exploring the Internet for fun or profit
- ◆ Establishing communications with third parties
- ◆ Research for personal or business purposes
- ◆ Forwarding or transmitting information to third parties or employees
- ◆ Copying programs, files, and data
- ◆ Transmitting important, confidential, or proprietary information
- ◆ Speaking on behalf of the County

Filtering Services

Filtering services were added to the County to monitor and block out any inappropriate site(s). The filtering tool allows the County transparent monitoring, reporting and traffic management of all Internet sites from the County's internal network to the Internet. The purpose of this tool is to conserve network bandwidth resources, reduce legal liability, and boost employee productivity and to help enforce Internet access policies. The filtering services software is updated and new sites are added to the database daily. The filtering software automatically downloads updates to the database every night to ensure that the County is keeping up with the rapid evolution of the Internet.

Individuals needing access to certain blocked sites on the Internet due to job necessity must do so with written authorization from the Elected Official/Department Head or the Information Technology department.

Individuals that have received approval to transmit information on the Internet should understand that such transmissions are identifiable and attributable to the County. Disclaimers such as "***The opinions expressed do not necessarily represent those of the County,***" while a good idea, do not necessarily relieve

the County of liability. The Internet should be considered a public forum for all transmissions. All communications on the Internet provide an opportunity for a permanent electronic record, and can be edited and retransmitted. Accordingly, maintain a professional decorum in all communications and transmissions.

The following actions are prohibited under any circumstances:

◆ Portraying yourself as someone other than who you are, or the County you represent
◆ Accessing inappropriate web sites, data, pictures, jokes, files, and games
◆ Inappropriate chatting, e-mail, monitoring, or viewing
◆ Harassing, discriminating, or in any way making defamatory comments
◆ Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes
◆ Gambling or any other activity that is illegal, violates County policy, or is contrary to the County's interests

Business Reputations

Please keep in mind; a statement or posting of information on the Internet can cause serious damage, because information can be quickly and effectively disseminated. The County, and the law, can and will hold you responsible for offensive, discriminatory, and defamatory statements, or any other illegal activity.

Remote Access

Users are required to **turn off dial-up modems** at the end of the day. Modems must be programmed to pick-up after the fourth ring (this will help prevent unauthorized access). Users are required to turn off remote access programs within a reasonable time after use, usually 5 to 10 minutes. Downloading or uploading confidential or proprietary information requires approval by Elected Official/Department Head or the Information Technology department.

E-mail

All county personnel, with computer network accounts, will have access to the email system for the purpose of sending and receiving **internal email messages only**. The default email access will allow a user to communicate with other county employees but will not allow email messages to be sent to, or received from, email accounts **outside** of the Collin County network (external).

Any county staff requiring e-mail capability outside (external) of the Collin County environment must have the account access requested in writing, either via hard copy memo or an electronic request, from the Elected Official/Department Head to the Director of Information Technology.

All e-mail accounts are given standard names that are assigned by the Information Technology department. Personal use of e-mail is a privilege, not a right. Abuse of the privilege may result in appropriate disciplinary action. The content and function of an e-mail message determines if the e-mail is a local government record as well as its retention period. Recorded e-mail messages that fall under the definition of local government records are the property of Collin County and therefore the taxpayers of the county. Thus, they are subject to the requirements of the Texas Public Information Act and the laws applicable to local government records retention.

Elected Officials/Department heads are responsible for ensuring that their employees follow this policy.

Electronic Communications

E-mail is a wonderful tool. Used correctly, it can provide significant efficiencies, and improve the quality of the way we do business. It makes dissemination of information easy and cost-effective. Please take full advantage of it.

Uses that waste limited resources. For example, don't send chain letters, even for noncommercial or apparently "harmless" purposes, as these, like email with large graphic attachments and "junk e-mail", use up limited Network capacity resources. Only copy others on an e-mail who should be "in the loop" on that e-mail. Be careful with distribution lists, determining first whether it is appropriate for everyone on that list to receive the e-mail. Do not send "all hands" e-mails without first obtaining permission from the Elected Official/Department Head and Information Technology.

The same standards of decorum, respect, and professionalism that guide us in our face-to-face interactions apply to the use of e-mail.

Incidental or occasional use of e-mail for personal reasons is permitted. However, only County personnel are allowed access to the County e-mail system. The following e-mail activity is prohibited:

- ◆ Accessing, or trying to access, another user's e-mail account
- ◆ Obtaining, or distributing, another user's e-mail account
- ◆ Establishing and/or using unauthorized alias e-mail names/accounts
- ◆ Using e-mail to harass, discriminate, or make defamatory comments
- ◆ Using e-mail to make off-color jokes, or send inappropriate e-mail to third parties
- ◆ Transmitting County records within, or outside, the County without authorization
- ◆ Transmitting junk mail, chain letters, or soliciting for commercial, religious, charitable, or political causes

Employees are required to report inappropriate use of e-mail.

Appropriate e-mail etiquette is essential to maintaining a productive and professional work environment. Comments that might be made at parties, in

elevators, and on the telephone are now done via e-mail. However, e-mail does not disappear into thin air. It can be widely, easily, and quickly disseminated. E-mail can be edited, forwarded, distributed, and filed for later use, possibly at the most inopportune time. For professionals with electronic recovery skills, e-mail is a gold mine. If you would not put it in a memorandum on County letterhead, do not say it with e-mail!

Forwarding Information

E-mail makes attaching files and forwarding data a snap. However, the damage from forwarding something to the wrong person may be serious. Please take a minute to think through the appropriateness of all the parties you are forwarding. If you receive an e-mail (particularly e-mail with an attachment) and intend to forward it to others, consider the following:

◆ Is any of the information unnecessary or inappropriate for any individual? ◆ Would the author take exception to, or be embarrassed by, your forwarding the information? (A good rule of thumb is to copy the author.) ◆ Might the information be received negatively? ◆ Might the information be misunderstood? ◆ Is the receiver likely to forward the information to individuals that should not have, or do not need, the information? ◆ Do the attachments have viruses? If the answer to any of these questions is yes, do not forward the information. Edit it, or create a new file. A bad decision only result in misunderstanding, hurt feelings, and added work.

Spam

Sending unsolicited messages or files to individuals, groups or organizations that you do not have a prior relationship with is prohibited, without written authorization from the County. Sending messages or files with the intent to cause harm or damage to the intended receiver is a violation of County policy and will be prosecuted to the full extent of the law.

The Information Technology department filters all incoming email messages in an effort to protect the County from the countless number of spam mail messages, some of which can be sent with the intent to cause harm. While this filtering process is highly effective for stopping spam messages from known spamming sites and messages containing keywords common to spam messages, no filter will be 100 percent accurate all of the time. Unwanted mail messages from outside organizations may be reported to the Information Technology Help Desk.

Intranet

The County Intranet, like e-mail, is a wonderful tool. It can provide significant efficiencies; and it makes dissemination of information easy and cost-effective. As with **internal email access**, all county personnel with computer network accounts will have access to the Collin County Intranet. The default Intranet access will allow a user to access the information and programs posted to the county Intranet for the purpose of more efficiently performing the assigned job duties. Data, programs, and other information are updated regularly on the Intranet. As such, it is your responsibility to ascertain that information you are working with is current.

The same standards of decorum, respect, and professionalism that guide us in the office environment apply to the use of the Intranet. Important, confidential, and proprietary information is stored on the Intranet. Accordingly, only County personnel are allowed access to the Intranet, with written authorization from the Elected Official/Department Head or the Information Technology department. All County policies apply to use of the Intranet. The following activities are prohibited, without management authorization:

◆ Installation of a web site, page, or any other information ◆ Installation of business or personal software on the Intranet ◆ Exceeding authorized access of Intranet programs, data, and files ◆ Assisting anyone outside the County in obtaining access to the Intranet ◆ Making any changes to the Intranet hardware or software

Any county staff requiring Internet capability (i.e., outside of the Collin County environment) must have the account access requested in writing, either via hard copy memo or an electronic request, from the Elected Official/Department Head to the Director of Information Technology.

WEB Site

The Collin County web site is a useful tool that provides an additional means for departments to communicate with and provide service to the citizens of Collin County.

Under the authority of the Commissioners Court and the Internet Committee, all departments have the opportunity to establish and maintain a department web page within the County web site. The Internet Committee and Information Technology department has overall responsibility for ensuring the consistency and quality of the overall Collin County web site.

Departments are responsible for ensuring that the content on their web pages is accurate and kept current.

All changes to department web page content will be reviewed, approved and published to the production web site by the Information Technology department.

Local Area Network

All important, confidential, or proprietary information must be stored on the LAN. The LAN is equipped with electronic and physical security. Activity on the network is monitored for tampering and other security breaches. Maintenance and backup are performed on the LAN daily; and programs and other information are updated regularly. Use the LAN! It is safe, effective, and reliable. Because important, confidential, and proprietary information is stored on the LAN, only County employees are allowed access, without written authorization. All County policies apply to the LAN. The following activities are prohibited, without the authorization of the Elected Official/Department Head or the Information Technology department:

◆ Installation of business or personal software on the LAN ◆ Making any changes to the LAN hardware or software ◆ Accessing without authorization, or exceeding authorization, LAN programs, data, and files ◆ Assisting anyone within, or outside, the County in obtaining access to the LAN

Glossary of Terms

Computer Information

Data, software, files, and any other information stored on County computers and systems.

County (local Government) Record

Any document, paper, letter, book, map, photography, sound or video recording, microfilm, magnetic tape, electronic medium or other information recording medium, regardless of physical form or characteristic and regardless of whether public access to it is open or restricted under laws of the state, created or received by a local government or any of its officers or employees pursuant to law, including an ordinance, or in the transaction of public business. (Local Government Code §201.003(8)) The term does not include (a) extra identical copies of documents created only for convenience of reference or research, (b) notes, journals, diaries, and similar documents created by an officer or employee of the local government for the officer's or employee's personal convenience, (c) blank forms, (d) stocks of publications, (e) library and museum materials acquired solely for the purpose of reference or display, (f) copies of documents in any media furnished to members of the public to which they are entitled under Chapter 552, Government Code or other state law, and (g) any records, correspondence, notes, memoranda, or documents other than a final written agreement described by Section 2009.054(c), Government Code

Electronic media

All media capable of being read by a computer including computer hard disks, magnetic tapes, optical disks, or similar machine-readable media.

Electronic Record

The information that is maintained in electronic format in a computer for computer processing and the product of computer processing of that information that satisfies the definition of "local government record data" in the Local Government Code §205.001.

Encryption

The process of turning plain text into cipher text by applying an algorithm that rearranges or changes its input into something unrecognizable.

Firewall

A specifically configured system that serves as a secure gateway between an outside network (e.g., the Internet), and the organization's internal networks.

Hacker

Slang, an individual intensely absorbed with and/or extremely knowledgeable about computer hardware and software. Also used to describe those who break into and corrupt computer systems. (Hacker is used here to describe those who break into and corrupt computer systems.)

Hot Links

A connection made between application programs so that when changes are made to the data in one file, the changes appear instantly in another.

Intranet

A local area network which may not be connected to the Internet, but which has some similar functions. Some organizations set up World Wide Web servers on their own internal networks so employees have access to the organization's Web documents.

Internet

The mother of all networks. A group of networks connected via routers.

ISDN

Integrated Services Digital Network. Digital telecommunications lines that can transmit both voice and digital network services, and are much faster than the highest speed modems.

LAN

A set of connections between computers that provides the basis for electrical transmissions of information, generally within a small geographical location to serve a single organization.

Local government record data

The information that by law, regulation, rule of court, ordination, or administrative procedure in a local government comprises a local government record as defined by Local Government Code, §205.003.

Login

A start-up file stored in the user's directory. This file is used to execute commands that should only be executed at login time, such as establishing the terminal type and starting windows systems.

Modem

Short for modulator-demodulator. A hardware device that allows two computers to communicate over ordinary telephone lines.

RAM

Random Access Memory. The working memory of the computer. RAM is the memory used for storing data temporarily while working on it, running applications programs, etc. "Random Access" refers to the fact that any area of RAM can be accessed directly and immediately.

Server

A computer or device that administers network functions and applications.

Spam

Generally defined as an unsolicited mailing, usually to many people

Transitory Information

Records of temporary usefulness that are not an integral part of a records series, that are not regularly filed within a recordkeeping system, and required only for a limited period of time for the completion of an action by an employee or official; not essential to fulfillment of statutory obligations or document departmental functions.

Trojan horse

A program that masquerades as something it is not, usually for the purpose of breaking into an account or exceeding commands with another user's privileges.

Virus

A set of instructions that can reside in software; and can be used to destroy other files or perform other tasks with another user's privileges.

Web Site

A server computer that makes documents available on the World Wide Web. Each web site is identified by a host name.

Worm

A program that propagates by replicating itself on each host in a network, with the purpose of breaking into systems.