2007 FANNIN COUNTY

GENERAL RULES DETAILED INSIDE

Personal Files

Personal Safety

Software Usage

System Security

Illegal Activities

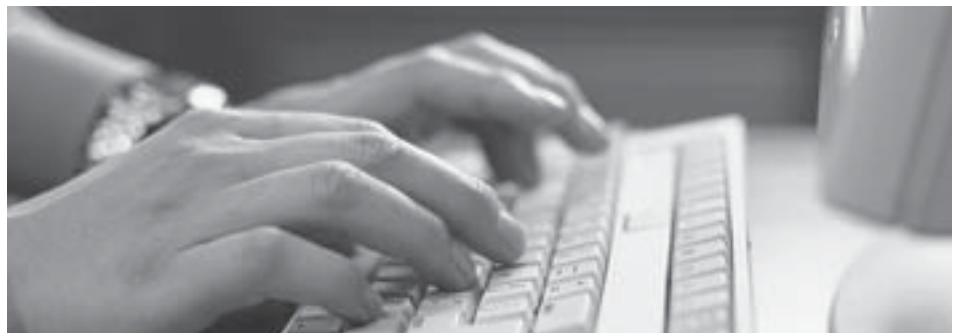Inappropriate Access

Copyright Infringement

Inappropriate Language

Respecting Resource Limits

County Web Site Procedures

Our Web Site
www.co.fannin.tx.us

ACCEPTABLE USE OF COMPUTERS POLICY

Fannin County is very pleased to bring Internet access to its county employees through the county network, believing the Internet offers vast, diverse and unique resources to its users. Our goal in providing this service is to promote excellence in our county offices by facilitating resource sharing, innovation, and communication. This document is to notify county employees about the network and the policies governing its use.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of intellectual value in the context of a workplace setting.

On a global network, it is impossible to control all material, and an industrious user may discover controversial information. Fannin County firmly believes the valuable information and interaction available on this worldwide network far outweigh the risk that users may procure material inconsistent with the goals of the county.

Life is a series of choices and consequences. If an employee chooses to use these resources for finding information that will be of assistance in completing a task, the benefit will be continued access to the Internet.

If a Fannin County employee chooses to access resources that are objectionable, such adult-oriented or restricted content, the consequence will be suspension or termination of access privileges in addition to other sanctions outlined in Fannin County personnel policies.

County Employee Internet Access

Limited electronic mail communication with people all over the world

Information and news from government sources, research institutions, and other sources

Many public and private libraries, the Library of Congress, and the Educational Resources Information Clearinghouses (ERIC), which store, update, and share thousands upon thousands of articles on endless topics

Rules of General Internet Use

* Never give out personal information, especially your full name. First names only are best. Never give anyone your home phone number, home address, or other data anywhere on the Internet.
* Be concerned about getting email messages from anyone asking you for personal information, attempting to arrange secret meetings, or engaging in other activities which might suggest a problem or an unsafe condition.
* Always ask for permission to use pictures or text from someone's online site, then give the person credit in your bibliography.
* Treat other online users as you would like to be treated.
* Treat county computers respectfully.
* Protect your password if you have been given one. Never send password information to any one in an email.
* While online, stay focused on the work-related topic you are researching. The Internet is an excellent resource—use it responsibly.
* Ask for help if you are having problems. Write down any error messages that appear when you try to do something.
* Keep the area around your computer clean and free of food and drink.
* Never use your computer with the intent to harm others.

Policy guiding the use of the Fannin County network

1 Personal Safety

Users will not post personal contact information about themselves or other people. Personal contact information includes, but is not limited to home, school, and work addresses and telephone numbers.

Users will not re-post a message that was sent to them privately without permission of the person who sent the message.

Users will promptly disclose to their supervisors any messages they receive that are inappropriate or make them feel uncomfortable.

To avoid unnecessary and unsolicited intrusion into the privacy of everyone in our system and the very system itself, users will not directly access any "chat room" through any computer on the Fannin County network. Making a connection to such sites does not happen by accident, but should anyone unintentionally find him/herself in a "chat room" site through some other connection, that person must immediately disconnect from that site.

2 Illegal Activities

Users will not attempt to gain unauthorized access to the county system or to any other computer system through the county network or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing".

Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means.

Users will not use the county equipment to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, and/or threatening the safety of others.

3 System Security

Users are responsible for their own individual accounts and computers and should take all reasonable precautions to prevent unauthorized access. Under no conditions should a user provide his/her password to another person other than the IT department.

Users will immediately notify the system administrator or their supervisors if they have identified a possible security problem. Users will not themselves look for security problems because this may be construed as an illegal attempt to gain access.

Users will avoid the inadvertent spread of computer viruses by following the county virus protection procedures for downloading information or software. See article 11 of this document.

4 Inappropriate Language

Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.

Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

Users will not engage in personal attacks, including prejudicial or discriminatory attacks.

Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending those messages, he or she must immediately stop.

Users will not knowingly or recklessly post false or defamatory information about a person or organization.

5 Respecting Resource Limits

Users will use the system only for professional or career development activities and, on a limited basis, high-quality self-discovery activities.

Users will not download large files unless absolutely necessary. If necessary, users will download the file at a time when the system is not being heavily used and immediately move the file from the system computer to their personal computers.

Users will not post chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary messages to a large number of people.

Users will check their e-mail frequently and delete unwanted messages promptly.

Users will subscribe only to high-quality discussion group mail lists that are relevant to their professional career development.

Users are expressly prohibited from listening to streaming internet based radio broadcasts or watching streaming video. This activity uses an excessive amount of limited county bandwidth and slows the system unnecessarily.

6 Plagiarism and Copyright Infringement

Users will not plagiarize works they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user or presenting them without proper credit to the originator.

Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If users are unsure whether or not they can use certain works, they should request permission from the copyright owners.

7 Inappropriate Access to Material

Users will not use the county computers to access material that is profane or obscene, that advocates illegal acts, or that advocates violence or discrimination towards other people. Pornography and hate literature are two common examples of zero-tolerance access. For certain employees, a special exception may be made if the purpose of such access is to conduct a criminal investigation, and this special access requires prior approval from department supervisors and the county IT department.

If users inadvertently accesses such information, they should immediately disclose the access to their supervisors. This will protect users against allegations of intentionally violating the Acceptable Use Policy.

8 Personal Files and Information

Fannin County employees are expected to respect their coworkers' right to privacy and confidentiality. Employees should be aware of the following limitations that apply to the privacy of files, documents, email, and other electronically stored or transmitted materials:

> All messages, documents or files stored in or sent through a Fannin County computer or email communications systems are the property of Fannin County.

> All messages, documents or files stored in or sent through a Fannin County computer or email communications systems are to be used with professional conduct while being of appropriate content. Any misuse of these forms of communication will be a matter for discipline set forth in Fannin County personnel policies.

> When any files in a user's directory or email box are viewed by system administrators, the user will be notified except during an official investigation of possibly illegal activities.

> Systems administrators are authorized to examine user files to handle emergencies such as virus infestations and system crashes.

To properly maintain and manage this information and systems, the IT department and system administrators reserve the right to examine all data stored in or transmitted by these systems.

8 Personal Files and Information , continued

Fannin County computer and communications systems must be used for business and   educational purposes only. Incidental personal use is permissible only if the use does not consume more than a trivial amount of resources that could otherwise be used for organizational purposes and does not interfere with productivity or education. Permissible incidental use of an electronic mail system would, for example, involve sending a message to schedule a personal appointment. Messages relating to or in support of illegal activities may be reported to the authorities.

Users of the Fannin County computing and communications systems must not use these facilities for soliciting business, selling products, or otherwise engaging in commercial activities.

Fannin County information, including but limited to databases, mailing lists, internal software, and computer documentation, must be used for only the purposes specifically allowed by the department supervisor. Use of these information resources for any other work-related reason will be permitted only after the supervisor has granted permission in writing.

Fannin County software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-Fannin County party for any purposes other than purposes expressly authorized by the department supervisor or the Fannin County Judge.

Computer equipment provided by Fannin County must not be altered or added to in any way, including but not limited to upgrading the processor, expanding memory, or adding circuit boards without prior approval of the IT department.

9 Software Usage

Employees will only use county-approved and owned software such as Ableterm, Adobe Acrobat Reader, Adobe Page Maker, Dreamweaver, Fireworks, Flash, Internet Explorer, Microsoft Office, Symantec Anti-Virus, Outlook, Outlook Express, Paint Shop Pro, Print Shop, Word Merge, and WinZip.

Supervisors and the county IT dept. must approve all software. The use or installation of unapproved software is expressly prohibited.

End-users are not authorized to install unnecessary software including, but not limited to:

Peer2peer file-sharing such as LimeWire

Media players such as RealPlayer

Games

Personal programs such as Turbo Tax

Specialized screen savers

System tray programs such as Precision Time, Gator, and Weather Bug

Any software purchased, received via email and/or downloaded from the Internet

9 Software Usage, continued

Fannin County requires strict adherence to software vendor license agreements and copyright holder notices.

If an employee makes an illegal copy of program software, he or she is violating policy, and will be open to disciplinary action.

Fannin County allows reproduction of copyrighted material only to the extent legally considered "fair use" or with the permission of the author /owner.

Unnecessary software can be removed by the IT department or system administrator without prior warning to the user. If additional software is needed for county operations on a particular computer, it will be installed by IT support staff.

10 County Web Site Procedures

Department heads are responsible in their respective areas for identifying required posts for the Fannin County Web site and providing this information in electronic format to the Fannin County IT Department. All posts require final approval by the Fannin County IT Department.

Allow up to seven business days for the information requested to be posted or modified on the Fannin County Web site.

Fannin County makes no warranties of any kind, whether expressed or implied, for the service it is providing. We assume no responsibility or liability for any phone charges, line costs, or usage fees, nor for any damages users may suffer. This includes loss of data resulting from delays, non-delivery, or service interruptions caused by accident, user errors or omissions. Use of any information obtained via the Internet is at your own risk. We specifically deny any responsibility for the accuracy or quality of information obtained through the technology.

11 Fannin County Virus Protection Protection Procedures

Do back-up all important files on your computer(s) and keep a copy in a location other than the computer location, preferably a safe deposit box.

Never, never, never open an attachment on an email from an unknown source. Delete the email immediately.

Even with E-mail from someone you KNOW, DO NOT open attachments unless and until you have separate information from that source as to the type of attachment and it's contents. Even then, do not open it unless you have up-to-date anti-virus software properly installed on your computer. Doing so could lead to loss of data.

11 Fannin County Virus Protection Protection Procedures

Certain spread sheets and other program or executable files attached to E-mails can contain viruses of which the sender is NOT aware. So take no comfort if your friend tells you an attachment did not damage their computer; Virus actions are frequently RANDOM.

If you visit Web Sites linked in an unsolicited email message, those Web Sites frequently collect personal information from your computer which, at best may cause you to be placed on more junk email lists, and at worst can steal credit card and other personal information stored on your computer. Many such programs ONLY require that you click a button, usually marked "ENTER" to start this clandestine information collection process.

If you have responded to random "Chain" emails in the past, whether for prayers or for the hope of winning money or vacations, please STOP. Terrorists and their supporters can easily use such tools to create millions of false trails for authorities to follow, thus thwarting efforts to locate and bring them to justice. Likewise, remove any unknown or outdated E-mail addresses from your E-mail address book.

Don't ever respond to an E-mail that offers to "remove you from an E-mail list". They are usually simply verifying your E-mail address so they can sell it to others for more money.

Do install anti-virus software and update it every two weeks, or at minimum, once each month. The installation is done by the IT department and it is setup to automatically update each week.

Use only software updates available from legitimate Vendor Website downloads such as Windows Update. Never download software offered in an unsolicited email or website, unless you check with your department head or the IT department to make sure it is from a legitimate source.