Macon County

Employee Computer Policy

The purpose of the **Employee Computer Operating and Security Policy** is to help protect the County and employees of the County from liability and business interruptions due to inappropriate use of County computers and/or breaches of computer security.

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 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 in which you are not certain, inquire of management.

The content of electronic data (including Email) sent, received or created by the County, is considered public record by the North Carolina General Statutes. This data is therefore subject to State guidelines for retention, disposition, and destruction as public records.

Employee Computer Operating and Security Policy

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, damage, or theft of computer information and equipment. This includes all offsite computer equipment and software.

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.

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. It is not uncommon for employees to try to figure out a friend’s, or associate’s, 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. If you have a question about password selection or safekeeping, please see your supervisor or the Information Technology Manager.

Password Access Program

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). Report any irregularities flagged by the password access program (last login time and date, number of attempts to login, etc.). Turn off your computer when you leave at night. 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 management. Watching other users enter information, and looking at computer disks that do not belong to you, is prohibited. Obtaining, or trying to obtain, other users' passwords, or using programs that compromise security in any way, are violations of County policy.

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 management. 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 management.

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, see the Information Technology Manager.

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, contact Information Technology even if Antivirus software offers to clean it up.

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 without prior management approval is prohibited.

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
- ♦ 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 departmental management and Information Technology management

If you observe a document at a shared printer, or any other location, do not read it without permission.

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. Turn off 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.

Administrative Matters

Back-up

Users are responsible for regular back up of essential computer files, and secure storage of back-up disks. All backed-up files should be stored on a secure computer disk, tape or LAN Server, other than the one containing the original data.

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.

Copyright Infringement

The County does not own computer software, but rather licenses the right to use software. Accordingly, County licensed software may only be reproduced by authorized County officials in accordance with the terms of the software licensing agreements. Unauthorized copying, redistributing, and republishing of copyrighted or proprietary material are strictly prohibited. Copyright laws apply on the Internet as well.

Copies of shareware or “free” programs must be registered and approved by the Information Technology department. Shareware and free software often have licensing and use restrictions, and should not be copied or forwarded to others.

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. 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.

Accidents, Mistakes and Spills

Mistakes and accidents represent the biggest cost when it comes to computer information loss. 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. 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 management authorization.

Purchases of Computer Software and Equipment

Purchases of computer software and equipment are prohibited without approval from departmental management and Information Technology management. All computer software and hardware purchases including extended warranties and service agreements must be approved by the Information Technology department, meet pre-established quality requirements, and be compatible with other County computer software, equipment and service contracts.

Personal Use of Computers

Incidental and occasional personal use of County computers is permitted for reasonable activities. It is the employee’s responsibility to clear all personal use through their supervisor or department head.

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.

Separation of Employment

All information on users’ computers is considered County property. Deleting, altering, or sharing confidential, proprietary, or any other information upon separation requires management authorization. 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.

Internet Connections and Email

The same standards of decorum, respect, and professionalism that guide us in our face-to-face interactions apply to the use of e-mail. Appropriate e-mail etiquette is essential to maintaining a productive and professional work environment. If you would not put it in a memorandum on County letterhead, do not say it with 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.

Internet connections are authorized for specific business needs only. Connection to the Internet without management authorization is prohibited. Personal internet use is restricted to non-work hours such as authorized breaks, lunch hours, or before and after work as approved by the employee's supervisor. Work day personal internet use outside these times may subject employees to disciplinary action for misuse of County time and property. Furthermore, the following activities are prohibited without management authorization:

- Downloading information of any kind, including data, files, programs, pictures, screen savers, and attachments
- Transmitting important, confidential, or proprietary information
- Speaking on behalf of the County

Unapproved Activities

- 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

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 your supervisor. 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.

Remote Access

Remote access of computer systems is prohibited without prior approval.

LAN Access and Workstation setup

Users with access to local domain resources such as network printers, or file volumes are encouraged to use network resources. Network file resources are classified as single user and multi user. Single user file shares are for use by that user, and have that users name. Shared or multi user file shares are for all, or a group of users in that domain. Establishment of shared resources or resource connections should be authorized by Information Technology staff, who will assign the appropriate permissions for those resources ensuring a secure network environment. The following setup activities should be limited to Information Technology personnel.

Access to network resources
Mapping drives or printers
Sharing of network resources
Assigning workstation network configurations
Connecting equipment to the network

Computer Workstations and equipment will be unpacked and installed, and configured by IT staff.

Receipt of
Employee Computer Operating
and Security Policy

I have received and read the County's Employee Computer Operating and Security Policy. I understand that I am responsible for adhering to the policies and practices described therein. I understand that these policies may be added to, or changed by the County at any time. It is my responsibility to bring any questions I have about the Employee Computer Operating and Security Policy to my supervisor. I further understand that violation of this policy will be subject to disciplinary actions as outlined in the Macon County Personnel Policy.

____________________________ ________________
Employee Signature Date

____
Employee Name (Please Print)