

Cloud County Kansas Computer and Electronic Communications Policy

This policy governs the use of Cloud County's computer and electronic communications system, which includes telephone, voice mail, fax machines, Internet, electronic mail (e-mail), and other computer usage. Cloud County Employees and other Employees are encouraged to use the Cloud County's computer and electronic communications system to assist them in performing their work responsibilities effectively, efficiently, and at the highest level. Employees are to use e-mail and the Internet as they would any other type of Cloud County communications tools.

I. INTRODUCTION.

A. Scope and Purpose.

The computer and electronic communications system is the property of the Cloud County Kansas and shall only be used for valid purposes and other approved purposes. Permitted use will not (1) interfere with the Employee's work performance; (2) interfere with any other Employee's work performance; (3) compromise the integrity of the computer and electronic communications system; or (4) violate any other provision of this policy or any other policy, guideline, or standard of Cloud County. Use of the computer and electronic communications system is a privilege that may be revoked at any time.

Computer hardware/software owned or licensed by Cloud County is intended for business purposes and is to be used by Cloud County employees and elected officials for performing their official job duties. All communications and information transmitted, received, or stored in any Cloud County computer or electronic system belongs to Cloud County. Transfer of Cloud County files to an employee's personal computer remains the property of Cloud County.

B. Computer Policy Audits

Periodic audits should be conducted to ensure adherence to computer policies. Policies should be reviewed, evaluated, and adjusted if necessary.

C. Monitoring of Computer and Electronic Communication Usage

Cloud County has the right to monitor any and all aspects of its computer and electronic communication system, including, but not limited to, documents stored on Cloud County computers and/or networks, monitoring sites visited by Employees on the Internet, reviewing material downloaded or uploaded by Employees to the Internet, and reviewing e-mail and voice mail sent and received by Employees. This includes blocking access to certain Web sites for which access is deemed to be in conflict with Cloud County's policy. Such monitoring may be conducted without prior notice. Use of the Cloud County's computer and electronic communication system shall constitute consent to such monitoring.

Cloud County reserves the right to access and monitor e-mail use and any other computer related transmissions, as well as stored information, created or received by Cloud County

Employees with Cloud County Information Technology systems and resources under the following circumstances:

1. Performance monitoring or problem solving purposes;
2. Necessary in the course of an investigation for possible violation of Cloud County policies;
3. There is reasonable suspicion that a Employee has committed, or is committing a crime against Cloud County or for which the Cloud County could be liable;
4. Random or automated monitoring to ensure that content is in compliance with the County's established policies;
5. Request for monitoring is made by appropriate authority;
6. Required to do so by law.

The reservation of this right is to ensure that public resources are not being wasted and to ensure Cloud County's information systems are operating as efficiently as possible in order to protect the public's interests.

II. ACCEPTABLE USE POLICY.

This section provides guidelines for appropriate and inappropriate use of the Internet by Employees accessing the Internet from Cloud County premises and/or through Cloud County furnished computers, networks, or telecommunications facilities. Internet access is a resource provided by Cloud County for Employees to perform their Cloud County job responsibilities, and to enhance their ability to conduct the Cloud County's business. Internet use that is job-related fulfills these purposes and constitutes proper use; other use is prohibited.

A. Acceptable Uses of Internet Access.

Acceptable uses of the Internet depends on the specific business needs of your department with respect to obtaining and distributing information, and on your department's policies regarding the use of Employee time and Cloud County's resources. Some general examples of acceptable use include the following:

- searching the Internet for information relating to a current project required by your job duties;
- searching for and downloading information for purposes of job-related training, for yourself or for others;
- sending and receiving e-mail messages to non-Cloud County personnel in the course of conducting Cloud County business (such as contractors and consultants), provided that the messages do not contain confidential or sensitive Cloud County information;
- exchanging information with officials and Employees of other governments on topics related to your job functions;
- subscription, with the Information Technology (IT) Director's approval, to "listserv" and other information services that automatically deliver information that you need to conduct Cloud County business or perform your job duties.

B. Unacceptable Uses of Internet Access.

Under no circumstances, should Cloud County's computer and electronic communications system be used for sending, transmitting, receiving, copying, or storing any communication that is fraudulent, harassing, racially offensive, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate. Employees encountering or receiving this kind of material should immediately report the incident to their supervisor and the IT Director. Cloud County recognizes, however, that certain Employees may have valid business reasons to use the Internet to access otherwise inappropriate materials in the course of performing their duties. (Examples include, but are not limited to, criminal or administrative investigations of inappropriate Internet use, or use of the Internet by appropriate personnel to obtain health related information that includes depictions of the human body.) This section is not intended to preclude such use of the Internet.

Other prohibited uses of Cloud County's computer and electronic communication systems, include (1) sending chain letters; (2) sending copies of documents, messages, software, or other materials in violation of copyright laws; (3) compromising the integrity of Cloud County and its business in any way; (4) "moonlighting" or the advertisement of personal business; (5) soliciting and promoting political, charitable or religious causes; and (6) betting pools or other forms of gambling. Employees are cautioned to exercise care and good judgment when sending humorous material. Off-color humor in e-mail or voice mail is strictly prohibited. Moreover, humor, irony, and emotion are difficult to communicate in an e-mail message. Therefore, attempts at either may be misinterpreted by the reader or recipient.

Use of the Cloud County's Email and computer systems for union business or charitable causes must receive prior approval from the County Commissioners and may be revoked at any time for abuse or misuse.

In accordance with Cloud County policy, you may not use your Cloud County furnished Internet access or Cloud County furnished computers, networks, or telecommunications facilities to:

- promote political candidates or otherwise engage in political activity;
- participate in public debate on the Internet (including but not limited to "chat rooms" and bulletin boards) unless it is directly related to your job duties and has the approval of your supervisor;
- participate in public debate or information exchanges in a way that suggests your personal views are official views or policies of the Cloud County.

Conversely, it is a violation of Cloud County policy for any Employee to use Cloud County computer systems for the purpose of satisfying idle curiosity about the affairs of others.

Hacking is the unauthorized attempt or entry into any computer. Cloud County employees' must never make an unauthorized attempt to enter any computer. Such an action is a violation of the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. & 2510.

The representation of yourself as someone else, real or fictional, or a message sent anonymously is prohibited. Users of Cloud County's network must never send, post or provide access to any confidential Cloud County materials or information.

Software downloaded to Cloud County computers from the Internet may contain computer viruses or otherwise interfere with the operation of your computer or the operation of Cloud County networks. Cloud County software is licensed to Cloud County for Cloud County's use only and may not be made available for use by other than Employees. Employees who become aware of any misuse of software or violation of copyright law should immediately report the incident to the IT Director.

For these reasons, you may not knowingly use Cloud County computers or your Internet access to:

- download software from the Internet;
- upload software owned by or licensed to Cloud County to any Internet site, Internet address, or external e-mail address; or
- transfer software over the Cloud County's e-mail system.

You are not permitted to access the Internet from Cloud County premises and/or through Cloud County furnished computers, networks, or telecommunications facilities for personal use (i.e. use for any purpose not directly related to the conduct of Cloud County business).

You may not use Cloud County equipment to access your personal (i.e., not Cloud County provided) Internet account, Internet service provider, or other on-line service without the approval of the IT Director. Such access creates the risk of inadvertently importing a computer virus or otherwise compromising system security. If you receive approval from the IT Director, you may use such access only for purposes that are directly related to the conduct of Cloud County business.

You may not subscribe to or request services that provide information through "push technology" -- i.e. by continuously delivering information to the Employee's Internet address automatically and without a specific request from the Employee -- unless the information transmitted by the service is directly related to your job functions, and use of the service is approved by the IT Director. This is because the large quantities of data transmitted by many such services can quickly exhaust the storage capacities of your computer and the Cloud County's network, and can even cause network failure.

III. CLOUD COUNTY KANSAS WEB SITE.

To preserve the public nature of the Cloud County's Web site and to avoid any perception that Cloud County endorses or provides favorable treatment to any private person or business enterprise, corporate or commercial logos or links to vendor sites will only be allowed on Cloud County's Web site with prior written approval of the Commissioners.

IV. DISCLAIMER OF LIABILITY.

Cloud County is not responsible for material viewed or downloaded by Employees from

the Internet. Employees are cautioned, that included among the massive amount of information on the Internet, some is offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid coming into contact with some of this material on the Internet, even when performing innocuous search requests. In addition, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Employees accessing the Internet do so at their own risk.

V. VOICE MAIL POLICY.

Departments are encouraged to use voice mail to serve both internal and external publics. Voice mail is never to be used as a mechanism for screening calls. Such action is subject to discipline. Each department is allowed to set up and enforce additional voice mail or telephone policies, which may be applicable to its activities. Such policies may not conflict with Cloud County policy.

Cloud County telephone numbers published to the telephone directory should not use voice mail as the primary means for answering the phone during business hours. Those phones may have the voice mail option for after hours and internal messages, but should always be answered by a "live" person during business hours, when possible.

The goal is to minimize the number of times a citizen gets connected with voice mail. Messages should reflect when the Employee is gone for more than that day (or else the phone should be forwarded to a live person). Calls should never be transferred from voice mail to voice mail.

The following are acceptable practices:

- Greetings placed on Cloud County voice mail must be kept current. If an Employee with voice mail privileges is out of town or away from the desk for an extended period of time, the message must reflect when a call will be returned.
- It is important that voice mail (incoming messages) be reviewed and responded to appropriately, usually by the end of the business day. Supervisors are responsible to ensure appropriate use by themselves and by the Employees they supervise.
- It is advised that every voice mail offer the option to the caller to push "0" for live operator/clerical assistant. Employees should ensure that the operator is aware that they may receive those calls.
- Voice mail messages (incoming and outgoing) should be business like and professional. Use of obscenity or other offensive languages is grounds for discipline.
- Employees should be aware that voice mail messages are being monitored.
- Individual voice mail, accounts may be accessed by a supervisor.
- There must be a "live-person" at the end of any calling cycle. Departments are also responsible to check their systems to make sure that no black holes exist and that calls roll over to a live answer during business hours.

VI. NETWORK PASSWORDS & PROTOCOL.

Cloud County employees shall not reveal their usernames and passwords (except to their Supervisor or staff members in the IT Department) or otherwise breach the security of the network. Passwords should be obscure and a minimum of six characters in length. For best security, passwords should include special characters (e.g., “@,” “!,” “&,” “%”). All passwords should be changed every 90 days. Employees of the network who do not change their passwords may be prompted to make a change or they may be automatically locked out of the system.

Cloud County employees should lock their computers whenever they leave their desk. Pressing the CTRL-ALT-DELETE keys will prohibit unwarranted access to Cloud County’s network. If computers are found unlocked and unattended, the IT Department may lock the user account preventing access to Cloud County’s network.

A. Antivirus Software

Antivirus software is the first defense against malicious computer programs that can damage workstations and servers. Antivirus software should be installed and maintained on every workstation and every server. Enterprise level virus protection that actively scans open files on the server(s) will be used. Antivirus software must be updated regularly. Enterprise level software should be configured to update itself automatically and “push” the updates to all workstations. If an auto-update server is not available, designated personnel should download updates manually and distribute them to all workstations and servers. Preferably, updates should be downloaded and applied weekly.

B. Deleted Files

Deleted files on workstations should be cleared from the “recycle bin” to ensure that they are not restored by unauthorized individuals.

C. Proprietary Information

Proprietary information refers to any sensitive material that should not be seen by anyone besides authorized personnel. This would include employees’ personal information, payroll information, financial records, etc. Proprietary information should be treated as private and kept hidden from the eyes of unauthorized personnel and the public. When a user leaves their workstation unattended, any screens that display proprietary information should be closed. When possible the workstation should be locked before leaving it. If this system will be left idle for an extended length of time, the user should logout of the network.

Proprietary information should be stored on the server in a directory separate from other departmental data. Access to that directory should be given only to the individuals who must use it to perform their work activities. Proprietary information should never be stored in a public or shared-access directory.

Proprietary information should never be transmitted across the Internet without encryption. This would include attaching a file to an email message, uploading via FTP, or uploading to a web-based file folder (i.e.: Yahoo Briefcase). Proprietary data should always be encrypted and password secured before being transmitted across an unsecured network.

VII. COMPLIANCE.

Violations of this policy may result in restriction or loss of Internet access, and are subject to the normal disciplinary procedures of the Employee's department for misuse of Cloud County resources and Employee time. Each department is responsible for enforcing compliance with this policy by its Employees. Any Employee who has experienced misuse of Internet access, including non-conformance to this policy, evidence of potential viruses, or unauthorized access, should immediately report it to his or her supervisor.

VIII. PRIVACY.

Cloud County may engage in monitoring of telecommunications systems and computer related activities, including electronic mail messages, data files, and locally installed software. Monitoring may be performed for valid business purposes, including employee supervision. All employees will be informed of monitoring policies and will be required to consent to such monitoring as a condition of employment. Monitoring for employee supervision reasons will be performed by the IT Department at the formal request of an appropriate manager (e.g., Department Head, Commissioners, etc.), and a record of the monitoring activities should be kept in the employee's personnel file. Monitoring requests associated with employee supervision will be documented. Forms of monitoring may include, but not be limited to, inspection of a user's local computer, inspection of data files created on the local computer and/or the network, inspection of email mailboxes, and use of network, internet, and/or email monitoring and filtering software.

Employees should not expect that their communications using Cloud County systems, including, but not limited to, communications involving e-mail and Cloud County-furnished Internet access, are private or confidential. Employees do not have an expectation of privacy, and waive their right of privacy, in their use of the computer and electronic communication system, including, but not limited to, the documents, e-mail and voice mail messages they create, store, send and receive, and the Internet sites they visit.

I understand that there will be a periodic inspection of my PC and network drives to insure compliance with these regulations.

Also all employees and elected officials waive any right to privacy regarding any document, file or communication they create, delete and store or receive in/on any Cloud County-owned computer-related equipment. This includes, but is not limited to: Personal computers, laptop computers, computer servers, cell phones, PDA cell phones such as Blackberry's and I-Phones and other such handheld equipment. Cloud County reserves the right to access and disclose, should it become necessary, documents regardless of format.

VIII. ISSUANCE AND CIRCULATION.

The Personnel Department is responsible for publicizing this policy to all employees by issuing a written copy of this policy to all Cloud County departments.

Cloud County, through its department heads, managerial and supervisory employees, will implement this policy.

A copy of this Policy will be given to all employees that utilize computers, E-mail and the Internet in the performance of their duties or have access to same.

The Cloud County Commissioners may, from time to time, establish guidelines, consistent with this policy, to insure the effective and efficient use of these resources.

This Computer and Electronic Communication Policy is adopted by a majority vote of the Cloud County Commissioners at their Regular Session of the August Meetings on Monday August 31, 2015.



Gary Caspers, Chairman



Bill Czapansky



Gail Engle

**Cloud County Kansas Computer and Electronic Communications Policy
Employee Acknowledgment**

I have read, understand, and agree to comply with all the terms of this policy governing use of the Cloud County Kansas's computer system. I understand that a violation of this policy may result in disciplinary action, including possible termination, as well as civil and criminal liability. I further understand that this policy may be revised, expanded, or otherwise modified at any time, and that it is my responsibility to ensure that I am familiar with the current Computer and Electronic Communications System Policy at all times. I further understand and acknowledge that I am bound by the terms of the policy regardless of whether or not I have signed this policy or any modification thereof.

Date _____

Signature

Printed name