Computer, Email, Internet, and Social Media Policy

Information Technology Department Policy

Effective Date: November 1, 2022

Approved by Cannon County Commissioner October 6, 2022

Information Technology Department
Computer, Email, Internet, and Social Media Policy

Contents

Computer, E-Mail, and Internet Usage

Cannon County recognizes that use of technology has many benefits for Cannon County and its employees. Computers, the Internet, and email make communication more efficient and effective. Therefore, employees are required to use these technologies appropriately. Unacceptable use of these things can place Cannon County and others at risk. This policy discusses acceptable usage of this technology. Cannon County intends to honor the policies set forth below but reserves the right to change them at any time.

Guidelines: The following guidelines have been established for using computers, the Internet, and email in an appropriate, ethical and professional manner. Exceptions may be made for individual job specific purposes.

1. Cannon County maintains computer network servers, an Internet server, and an electronic mail system. This system is provided by Cannon County to assist in the conduct of its business. The entire system, including the computers and anything on them and generated on them or with them, is the property of Cannon County. The system is not the private property of any employee. This means that anything created on a computer, generated on a computer, received by a computer, or put on a computer using Cannon County's system is the property of Cannon County.

2. The use of the system is reserved solely for Cannon County business.

3. Cannon County is entitled to know any passwords placed on any documents, files, or programs within the system, including passwords placed on documents, files, or programs by any employee. Any refusal may be grounds for disciplinary actions.

4. Cannon County will on occasion supply a laptop computer, tablet, or hand-held device to employees. These devices are also considered part of the system and are subject to the same rules, even if the devices are used at other places other than County property or on a different network. All computers, laptops and devices issued by Cannon County for general use are required to implement two-factor authentication. Two factor authentication provided by a third party service provider (such as Microsoft, Google or Local Government) is acceptable. Department heads should work with the IT Department to ensure that all members of their department are using two factor authentication at all times.

5. Cannon County computers, including its internet servers and network, the Internet, and email access may not be used for transmitting, retrieving or storing any communications of a defamatory, discriminatory or harassing nature or materials that are obscene, pornographic, or X-rated. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, political party, physical attributes, or sexual preference shall be transmitted. Harassment of any kind is prohibited.

6. Disparaging, abusive, profane, or offensive language; materials that would adversely or negatively reflect upon Cannon County or be contrary to Cannon County's best interests; and any illegal activities—including piracy, hacking, extortion, blackmail, copyright infringement, and unauthorized access to any computers on the Internet or email—are forbidden.

    a. Copyrighted materials belonging to entities other than Cannon County may not be transmitted by employees on the County's network. All employees obtaining access to other entities' or individual's materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission or as a single copy to reference only. If you find something on the Internet that may be interesting to others, do not copy it to a network drive. Instead, give the URL (uniform resource locator or "web address") to the person who may be interested in the information and have that person look at it on his/her own.

7. Do not use the system in a way that disrupts its use by others. This includes excessive usage, sending or receiving many large files and "spamming" (sending email messages to many users.)

8. The Internet is full of useful programs that can be downloaded, but some of them may contain computer viruses that can extensively damage our computers. Also, many browser add-on packages (called "plug-ins") are available to download. There is no guarantee that these plug-ins will be compatible with other programs on the network and they may cause problems; therefore, please do not download them without proper approval from the IT Department.

9. Each employee is responsible for the content of all text, audio or images that he/she places on Cannon County's computers or sends over Cannon County's internet and e-mail system. No email or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else. Also, be aware that Cannon County's name is attached to all messages so use discretion in formulating messages.

a. Email is not guaranteed to be private or confidential. All electronic communications are Cannon County's property. Therefore, Cannon County reserves the right to examine, monitor and regulate email messages, directories and files, as well as Internet usage.

10. Internal and external email messages are considered county records and may be subject to discovery in the event of litigation. Be aware of this possibility when sending email within and outside Cannon County. Additionally, do not dispose of or destroy such messages except in conformity with Cannon County's document retention policy.

Prohibited Use of Peer-to-Peer File Sharing

It is a violation of federal law to share and/or distribute copyrighted materials without the permission of the copyright holder. This is typically done through file-sharing software like BitTorrent, KaZaA, Emule, and Gnutella. File sharing software is most used to download music, movies, software and other media. This software may turn your personal computer into a server, or upload site, even if that was not your intent. Note: many worms, viruses and other malicious code get transferred during peer-to-peer file transfers, too. Use of these types of programs is strictly prohibited.

Limited Use of Social Networking Sites

County employees are strictly prohibited from using County owned computers and devices for the purpose of using or participating in social media and networking websites, including but not limited to, Facebook, Instagram, My Space, Linked-in, Snapchat, Tiktok, Twitter, Truth Social, YouTube and all other such similar internet websites unless allowed for official work purposes, as allowed by the Social Media Policy below.

Social Media Policy

Using social media at work

Employees may not use social media while on work time or on equipment provided by Cannon County except for work related purposes as authorized by your supervisor and the Cannon County Commission. Do not use a Cannon County email address to register on social media networks, blogs or other online tools utilized for personal use. Use of social media for official County purposes must be registered under a County email address, and logins, passwords/security information must be given to IT and HR. Wherever possible, the social

media account should be in the name of the County department and not an individual. Additionally, IT and the Finance Director must be made administrators or have administrative access to the social media account. Persons who are not Cannon County employees are not to be allowed to post as to appear as Cannon County, Cannon County officials or employees, nor to administer the account.

Use of social media on behalf of the County presents certain risks and carries with its certain responsibilities. To assist you in making responsible decisions about your use of social media, we have established these guidelines for appropriate use of social media.

Department heads, supervisors, and employees with access to County social media accounts should refer to the Social Media Management Guidelines for additional guidance in administering the policy, but the terms and conditions of these guidelines are applicable to all employees.

Social Media Management Guidelines

In the rapidly expanding world of electronic communication, social media can mean many things. Social media includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal website, social networking or affinity website, web bulletin board or a chat room, whether or not associated or affiliated with Cannon County, as well as any other form of electronic communication.

The same principles and guidelines found in Cannon County policies and procedures and the basic beliefs apply to your activities online. Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance, the performance of fellow employees or otherwise adversely affects citizens, suppliers, people who work on behalf of Cannon County or Cannon County's legitimate business interests may result in disciplinary action up to and including termination.

Know and follow the rules

Inappropriate postings that may include discriminatory remarks, harassment, political endorsements and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination.

Be respectful

Always be fair and courteous to fellow associates, citizens, suppliers or people who work on behalf of Cannon County. Also, keep in mind that you are more likely to resolve work-related complaints by speaking directly with your supervisor or co-workers than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, and threatening or intimidating, that disparage Cannon County citizens, customers, employees or suppliers, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion, sexual orientation, or gender identity or any other status protected by law or County policy.

Be honest and accurate

Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the Internet archives almost everything; therefore, even deleted postings can be searched. Never post any information or rumors that you know to be false about Cannon County or its citizens, fellow employees, suppliers, and people working on behalf of Cannon County.

Post only appropriate and respectful content

Maintain the confidentiality of Cannon County trade secrets and private or confidential information. Trade secrets may include information regarding the development of systems, processes, products, know-how and technology. Do not post internal reports, policies, procedures or other internal business-related confidential communications.

Do not create a link from your blog, website or other social networking site to a Cannon County website without identifying yourself as a Cannon County employee.

Express only your personal opinions. Never represent yourself as a spokesperson for Cannon County. If Cannon County is a subject of the content you are creating, be clear and open about the fact that you are an employee and make it clear that your views do not represent those of Cannon County, citizens, fellow employees, suppliers or people working on behalf of Cannon County. If you do publish a blog or post online related to the work you do or subjects associated with Cannon County, make it clear that you are not speaking on behalf of Cannon County. It is best to include a disclaimer such as “The postings on this site are my own and do not necessarily reflect the views of Cannon County.”

Retaliation is prohibited.

Cannon County prohibits taking negative action against any employee for reporting a possible deviation from this policy or for cooperating in an investigation. Any employee who retaliates against another employee for reporting a possible deviation from this policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination.

Media contacts

Employees should not speak to the media on Cannon County's behalf. All media inquiries should be directed to department heads/supervisors, and in turn they are to forward requests to the County Attorney's office.

Prohibited Use of Streaming Audio and Visual Media

County employees are strictly prohibited from using County owned computers and devices for the purpose of accessing non-employment related streaming audio and visual media and websites, including but not limited to, streaming music, radio, and video. The collective personal use of audio and visual media causes a significant drain on the County's Internet services and consequently impacts the ability of County employees to effectively use the Internet for employment related work. This policy is not intended to prohibit an employee's use of on-line training, or other such similar use of streaming media, that is directly pertaining to, related to, or required by an employee's work for the County. This policy is also not intended to prohibit an employee from listening to music or radio in the workplace, by and through personal audio devices that do not use the County's Internet for streaming media. It is also prohibited to store entertainment media on County computers. This policy applies to use of the County's public Internet access as well.

Cannon County's Right to Monitor and Consequences

All Cannon County-supplied technology, including computer systems and company-related work records, belong to Cannon County and not the employee. Cannon County routinely monitors usage patterns for its email and Internet communications. Although encouraged to explore the vast resources available on the Internet, employees should use discretion in the sites that are accessed. Since all the computer systems and software, as well as the email and Internet connection, are Cannon County-owned, all Cannon County policies related to such property are always in effect. Any employee who abuses the privilege of Cannon County-facilitated access to email or the Internet, may be denied access to the Internet and, if appropriate, be subject to disciplinary action up to and including termination.

At no time should the employees of Cannon County assume privacy of computer usage, email, or call records. Employees have no right to keep contents of email and files private.

GPS Monitoring and Tracking

County employees may, from time to time, be given the use of County property to perform their jobs. County property includes, but is not limited to, all equipment, vehicles, electronics, cell phones, and computers. Some County property that is issued to employees may contain GPS, or other such electronic tracking devices, whereby the County can track, locate, or determine the whereabouts of property and employees. The County reiterates that employees have no expectation of privacy in the use of County issued property. Electronic GPS monitoring or tracking information obtained by the County shall be retained in accordance with this policy, as is set forth herein above.

Questions Regarding the Use of the Internet or Email

If you have questions regarding the appropriate use of a computer, the Internet, or email, contact the IT Department (IT@cannoncountytn.gov).

Software Licensing and Support

All computer software and programs used at the County for institutional purposes must be licensed by Cannon County. Employees of the County are expected to follow the laws and regulations concerning the use of all programs purchased for and by the institution. Use of any program that is not properly licensed is prohibited and any violation of said agreement by County employees makes them personally liable and could jeopardize their employment with the County.

ANY AND ALL SOFTWARE THAT IS SPECIALIZED TO THE DEPARTMENT MUST BE APPROVED BY THE IT DEPARTMENT (IT@cannoncountytn.gov) AND THE DEPARTMENT HEAD.

Acquisitioning of Hardware/Software

All purchases of IT related equipment/software MUST first be reviewed by the IT Department. This applies even if the purchase is not made with IT allocated funds (i.e.: department funds, grants, etc.). ANY project that requires IT resources MUST be approved by the IT Department. This will ensure compatible equipment with the rest of the systems in the County, and future support.

Security

Phishing and Scams

Beware of fraudulent emails and websites that masquerade as messages from familiar institutions. By tricking you into disclosing your social security number, PIN number, a password, or an account number, identity thieves can drain your bank account or run up bills on your credit card. The best ways to avoid becoming a victim are:

- **Never disclose personal information in an email (i.e. credit card numbers, social security numbers)**
- Never click on the link in the email of items that are in question
- Always access the website by manually typing in the web address in a browser

Computer Security

What to Do if Your Computer Has Been Hacked or Infected

Disconnect your computer from the network, but do not unplug your machine. Contact your IT (IT@cannoncountytn.gov) administrator as soon as possible.

Passwords

Users are required to have their own password. Sharing passwords of any kind is strictly prohibited and may result in disciplinary actions. Any mal intent caused by the neglect of your username and password may also result in disciplinary actions. This includes a supervisor giving their password to a subordinate.

Passwords should be changed periodically. Requirements for passwords are not kept in this document due to security concerns. Please contact IT for specifications.

Electronic Record Retention

To the extent that County records are generated or retained as electronic or digital documents, the

records retention schedules applicable to other records in the County, i.e., the State of Tennessee[1], the Tennessee Open Meetings Act ("TOMA") and the County General Records Retention Schedule ("GRRS"), remain the same. In other words, simply because a document or record exists only in electronic or digital form does not make it immune from the records retention schedule, or any other requirement under TOMA. For instance, an agenda for a County council meeting is a record that must be retained for "2 years or until administrative need ends." In this instance, it does not matter whether the agenda exists in hard copy or electronic/digital format, the requirement to retain the record for "2 years or until administrative need ends" remains the same.

1.1 Email Retention. The County's position, for purposes of this policy, is that emailed messages are generally temporary or non-vital communications which should be discarded or deleted routinely. Despite the nature of these documents, emailed communications are subject to the record retention policies established in both TOMA, GRRS, and this County policy. In other words, County employees have the same responsibility to assess, define, and categorize email messages the same way they would any other County record, whether it be public, private, controlled, protected, or exempt from state laws.

1.1.1 Email Retention – Mailbox and Systems. County employees shall retain all incoming and outgoing emails until they are properly evaluated, defined, classified, and appropriately retained or deleted. Any email retained in an inbox for longer than one year should be audited by the employee. Based upon the audit, emails will be evaluated, defined, classified, and appropriately retained or deleted. Employees are subject to discipline for failure to periodically evaluate, define, classify, and retain or delete emails so that their inboxes are up to date. Employee email accounts belong to the County as the employer, and as such, employees have no right or expectation of privacy in County-based email accounts.

1.1.1.1 Personal Email Messages. The County discourages the use of employee email accounts for sending or receiving personal email messages.Employees that receive personal email messages on their County email accounts should immediately contact the sender and provide them with a non-employee email account in which to send email messages. In order to protect the County and the employee, personal email messages sent to County email accounts should be forwarded out of the account or deleted as soon as possible. Again, there is no right or expectation of privacy for any personal message or information received or sent through a County email account. The County email system shall be used for all business-related communication and no personal email address or system is permitted.

[1] Electronic Records Policy, State of Tennessee, October 2019

1.1.1.2 County Email Messages. County email accounts are intended only to be used in an employee's performance of County business. Email messages pertaining to County business should be retained within an employee account or mailbox until such time as the message, including any attachments, have been evaluated, defined, and classified. This policy recommends that employees review and clear their email accounts or mailboxes on a regular basis, but at least once each month. When reviewing and clearing email accounts, but prior to deleting any specific message, employees shall (1) print the email message, including any attachments, and save the hard copy to an appropriate file, or (2) save the hard copy to an appropriate drive. County email messages are not immune from the records retention schedules or TOMA, and in the event of a TOMA request from a member of the public, some email messages may require disclosure.

1.2 Electronic Document Retention. The purpose of this portion of the policy is intended to acknowledge the requirements of local, state, and federal law to maintain and preserve certain records, including electronic documents and records ("Electronically Stored Information" or "ESI"). County officials and employees must comply with these laws and this policy as it pertains to ESI. For purposes of this policy, there is no immediate distinction made between those documents which exist in "hard copy" and those which exist electronically; the retention and disclosure requirements of this policy, TOMA, and other such law or policies remain the same. The ESI policy and purpose is as follows:

1.2.1 This policy establishes guidelines and standards setting forth the requirements and responsibilities for the maintenance, storage, litigation holds, and destruction of County records which may be stored in digital, optical, magnetic, or any other such electronic and digital format.

1.2.2 All County departments and personnel shall adhere to this policy and the Cannon County Records Retention Schedule when storing or requesting the destruction of County records.

1.2.3 Records which are stored in an ESI format are held to the same retention requirements as "hard copy" records, and as such, an electronic record shall only be disposed of after it has fulfilled its purpose and met the required retention period that would be required of any other document.

1.2.4 ESI shall not be destroyed if a litigation claim, negotiation, audit, open records request, administrative review, or other action involving the record is initiated before the expiration of a retention period. In the event that any electronically stored record is subject to litigation, or potentially litigious dispute, the record shall not be destroyed until after the completion of the action

and the resolution of all issues that arise from it, or until the expiration of the retention period, whichever is later.

1.3 ESI Retention Schedule. The retention schedule for Electronically Stored Documents shall be no different from the record retention reschedule set forth in the GRRS. For purposes of this policy, there is no distinction made between the requirement to retain ESI records and documents and hard copy records and documents.

1.4 County Electronic Records. Electronic records and documents which must be retained in accordance with this policy, TOMA, and GRRS include, but are not limited to, any record created, generated, sent, communicated, received, or stored by electronic means on County email accounts or servers, as follows:

1.4.1 Records. Recorded information, regardless of medium or characteristics, made or received by the County, or any subdivision or department therein, that is evidence of its operations, and has value according to its classification, requiring its retention for a specific period of time. Recorded information, in any format, that is created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.

1.4.2 Electronic Records. Electronic records have these characteristics: authenticity (it is what is says it is); reliability (it can be trusted as a full and accurate representation of the transactions or facts); integrity (it is complete and unaltered); and usability (it can be located, retrieved, presented, and interpreted).

1.4.3 Electronic Record Formats. Electronic record common formats include, but are not limited to, text-based documents, databases, spreadsheets, web pages, drawings and diagrams, maps, electronic mail (email), etc.

1.5 County Electronic Record Exclusions. Electronic records and documents which do not need to be retained in accordance with this policy, TOMA, and GRRS include, and are otherwise excluded thereby, are as follows:

1.5.1 An entirely personal note or communication prepared or received by a County employee, that is intended to be unrelated to the County or County business. Again, this policy restates that there is no expectation of privacy in personal communications which are received, sent,

or otherwise transmitted, by and through County electronic or manual systems.

1.5.2 A temporary draft or similar material prepared for the originating employee's personal use or prepared by the originating employee for the personal use of an individual for whom the originator is working.

1.5.3 Material that is legally owned by an individual in the individual's private capacity and is otherwise unrelated to County employment or business.

1.5.4 Material to which access is limited by the laws of copyright or patent unless the copyright or patent is owned by the County or one of its departments or subdivisions.

1.5.5 Proprietary software.

1.5.6 Junk mail or other such related commercial publications received by a County.

1.5.7 Material that is cataloged, indexed, or inventoried and contained in the collections of a library open to the public, that is maintained in electronic format.

1.5.8 An employee's personal daily calendar, or other such personal note, prepared by the employee for the employee's personal use or for the personal use of another County employee or supervisor for whom the employee is working.

1.5.9 A computer program that is developed or purchased by an employee for his or her own personal use.

1.5.10 A note or internal memorandum prepared as part of the deliberative process by: (a) a member of the judiciary, (b) an administrative law judge, or (c) a member of any other body charged by law with performing a quasi-judicial function. If a question arises regarding the significance or classification of any such note or internal memorandum, employees should contact their immediate supervisor and/or the County attorney.

1.6 Procedures. The following procedures for the retention of Electronically Stored Documents within the County are as follows.

1.6.1 Retention Schedule. County records shall be retained pursuant to the current County General Records Retention Schedule ("GRRS"), prepared by the Utah State Archives, the current

Cannon County Records Retention Schedule, as well as all applicable state and federal record-keeping requirements.

1.6.1.1 Electronically Stored Information – ESI. The following information is included in the procedures for storing ESI.

1.6.1.2 Provision for adequate maintenance, disposal, and preservation of electronic records should be built into individual and departmental work processes and tools, so that electronic records management is a routine and time-efficient activity for all employees and/or records managers tasked with this responsibility.

1.6.1.3 Electronic records should be created and maintained in reliable and secure systems. The County departments shall identify systems or applications that create and maintain records. The development, modification, operation, and use of these systems/applications should be documented and coordinated with the IT Department to ensure reliability and security of records over time.

1.6.1.4 All County departments shall take appropriate measures to prevent unauthorized access to electronic records including, but not limited to logins, passwords, and other such electronic security codes and/or passwords.

1.6.1.5 Appropriate metadata about electronic records must be captured at the time of creation.

A. Context establishes who created the record and accurately identifies the transaction of which it was a part or to which it relates.

B. Electronic records should be created and maintained in reliable and secure systems. The County departments shall identify systems or applications that create and maintain records. The development, modification, operation, and use of these systems/applications should be documented and coordinated with the IT Department to ensure reliability and security of records over time.

C. All County departments and subdivisions shall take appropriate measures to prevent unauthorized access to electronic records, including the implementation of logins, passwords, security codes, and other such security measures.

D. Appropriate metadata about electronic records must be captured at the time of creation. Electronic data must be captured in such a manner as to document the context, content, and structure of electronic records: (1) Context establishes who created the record and the transaction of which it was a part; (2) Context is the actual data; (3) Structure is the format of the record. Structure must be captured so that the record can be migrated into the latest generation of hardware and software, as necessary.

E. In most cases, electronic records should be maintained in electronic form.

F. As technologies change, the County IT department is responsible for migrating ESI forward: (1) Records should be routinely monitored in order to identify any formats that are at risk of obsolescence.
(2) Migration of records should be planned, quality controlled, and documented; (3) Where records are in unique or legacy formats/systems with non-migration paths available, they must be supported by the County during their retention period, unless converted to a non-electronic format.

G. Digital records must be secure and tracked throughout the preservation process. The preserver should implement security measures to ensure that the records being preserved are not compromised during any preservation process.

H. Digital records preservation programs should be flexible. The preserver should seek to base digital records preservation approaches on non- proprietary technologies to avoid loss of control over County-owned information as a result of changed commercial arrangements in the future.

I. The original hardcopy of a permanent record (source document), that is converted into electronic format, can be destroyed after a minimum of 45 days have passed since the conversion, and the department is confident and has verified that the conversion of the records has been completely successful.

J. Electronic records shall be saved and stored on designated server-based personal and departmental workspaces or in a designated network database. These server workspaces fulfill the requirements of records retention, audit, and discovery since they are backed up, indexed, and can be centrally searched.

(1) Official electronic records shall not be permanently saved on any other media, including workstation hard drives, USB-attached memory devices, media drives, etc. Employees may from time-to- time have a need to temporarily store ESI on memory devices or drives, for employment purposes only, but such practices shall be used sparingly, and under no circumstances shall County records remain permanently on memory or media devices. All such devices, personal or County-owned, shall be turned into the IT Department for sanitization.

(2) Workstation hard drives are to be used only for the workstation operating system, County-licensed application program files, and associated temporary files appropriate to allow the workstation application programs to function correctly. Similarly, County-licensed programs shall not be transferred or converted for any employee's personal or home use.

1.6.2 Electronic Mail (email). In addition to the prior sections of this policy addressing the use and storage of emailed communications, the County adopts the following additional definitions, instructions, and policies pertaining to email.

1.6.2.1 Definition. Email is a means of sending messages between computer devices using an established network through the County's email system.

A. This information consists primarily of messages, but may also include attachments such as calendars, directories, distribution lists, word-processing documents, spreadsheets, and other electronic documents.

B. Email is stored in a digital format rather than on paper and is retrievable at a future date.

C. Due to format, email permits communication and transmission of up-to-date information like the telephone. Unlike current telephone features, email creates a record of the information that is being transmitted.

1.6.2.2 Retention Guidelines.

A. Follow the retention period for an equivalent hard copy record as specified in the County's approved retention schedule.

B. The record must be converted to a readable permanent format. If an email is determined to be an official record, the record to be retained shall be: (i) When the email originates from the County, the outgoing (sender's) copy of the email; (ii) The email containing the entirety of all the correspondence between all parties when an email thread has been created; (iii) The incoming (recipient's) email when originating from outside the County's government system.

C. Elected officials and administrative officers are responsible for instructing their employees in determining which email messages fall into retention categories, in using retention schedules, and in the process for destruction. Retention is the responsibility of the sender/recipient of the email, not the backup process.

1.6.2.3 Legal Considerations – Disclosure of Email

A. Public officials, administrative officers, and employees should keep in mind that email messages sent as part of their job assignments are not private and may be discoverable communications.

B. Since messages may be retained at different locations, users should

remember that their communication can be retrieved during a formal discovery process.

C. Discretion, therefore, is an important consideration when using this or any other technology to send, record, and/or retain communications.

D. Email – Neither Secure nor Confidential

(1) Electronically transmitted information travels through many networks and many different computer connections.

(2) This information is not secure, and should not be considered private.

(3) County departments are advised that there may be risk involved in using email to deal with confidential issues.

(4) Agents must be aware of all applicable statutory or regulatory requirements that would prohibit the disclosure of certain information: (a) Of special concern is the confidentiality of individually identifiable health and personnel information; and (b) Agents must be aware of this when transmitting this information by email.

1.6.3 Voicemail. Voicemail can be considered a type of electronic mail communication. In this case, the message is recorded in an audible rather than visible format.

1.6.3.1 Voicemail is primarily transitory in nature. Employees are encouraged to delete voicemail messages as soon as the messages are no longer needed. Employees are also encouraged to clear all voicemail messages within ten (10) days after the message date.

1.6.3.2 Employees wishing, or required by this policy, to retain information contained in voice mail messages shall save the voicemail in a specified folder on the voicemail server or may copy the desired information onto a network drive. A voicemail retained in a specified folder on the voicemail system or a network drive may be deleted at any time, unless subject to a hold directive issued pursuant to this policy. All messages subject to a hold directive shall not be deleted, altered, or destroyed until written authorization has been received.

1.6.3.3 From time to time, and as determined necessary by the County IT Department,

the County may delete and clear the voicemail system, including individual employee voicemail boxes. If the County determines to delete and clear the system, the County will provide employees with five (5) business day advance written notice that the voicemail system will be deleted and cleared. Upon receiving such notice, employees shall identify and retain those voicemail messages that are required to be retained, as is set forth herein.

1.6.4 Electronic Personnel, Discovery, and Litigation Holds. Electronic discovery refers to the discovery of electronic documents and data. Electronic documents include email, web pages, word processing files, computer databases, and virtually anything that is stored on a computer. The same rules that govern paper documents govern electronic discovery.

1.6.4.1 The obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatening litigation.

1.6.4.2 Upon determining that litigation or an investigation is threatening or pending and has triggered a preservation obligation, the County Attorney's Office shall take reasonable steps to communicate to affected persons the need for and scope of preserving relevant records (both electronic and hard copy).

A. An appropriate notice shall be effectively communicated to an appropriate list of affected persons.

1. The notice shall be sent to those departments and employees reasonably likely to maintain documents relevant to the litigation or investigation.

2. Notice shall also be sent to a person or persons responsible for maintaining and operating computer systems or files that have no custodian or owner but may fall within the scope of the preservation obligation.

B. The notice need not be a detailed catalog of information types to be retained. Instead, it should sufficiently describe the kinds of information that must be preserved so the affected custodians of data can segregate and preserve identified files and data.

C. The notice shall not trigger preservation of all documents, only those affected by the preservation obligation.

1.6.4.3 All County employees notified of the responsibilities to preserve documentation, electronic or otherwise, shall comply with all requirements contained in the notification.

A. When preservation obligations apply to documents and data spanning a significant or continuing time period, organizations should analyze whether special steps are needed to deal with hardware that might be retired if it contains unique relevant documents.

B. The preservation obligation, except in extreme documented circumstances, shall not require the complete suspension of normal document management policies, including the routine destruction and deletion of records not subject to the hold directive.

1.6.4.4 All documents and information subject to a hold directive shall not be deleted, altered, or destroyed until written authorization has been received by the holder of the records in question. Any existent hold shall be reviewed on an annual basis by the County Attorney's Office and the IT Departent.

1.6.5 Responsibilities:

1.6.5.1 Each County department and all County employees are responsible for compliance with County policies, including this policy relating to electronic records retention, maintenance, and destruction.

1.6.5.2 Compliance by the IT Department is subject to budgeting constraints and specifically includes:

A. Developing a security program for electronic records that follows federal, state, and local legal requirements.

B. Developing capability for preserving any electronic County record resident in the system for its full retention period; or, there must not be any system impediments that prevent migrating the record to another electronic records system, in as complete a form as possible.

C. Coordinating the documentation and destruction of electronic County records and disposing in a manner that ensures protection of any confidential information.

D. Maintaining proper climatic temperature control for any storage of electronic media.

1.6.5.3 Compliance requires a joint effort by all departments, Human Resources personnel, and the IT Department. Compliance includes:

A. Providing mandatory training during a regularly scheduled training cycle for users of electronic records systems in the operation, care, and handling of the information, equipment, software, and media used in the systems.

B. Developing and maintaining written documentation about institutional electronic records that is adequate for retaining, reading, or processing the records and ensuring their timely, authorized disposition.

C. Annual review and destruction of electronic records that have met the required minimum retention period or continued retention until destruction is operationally practical.

D. Media used to store electronic County records will be wiped (DOD wipe procedure) before the hardware passes out of the County's custody.

1.6.6 Destruction of Electronically Stored Information

1.6.6.1 When information that is stored electronically has fulfilled the retention period, the information can be erased.

1.6.6.2 The procedure and schedule for erasure is provided on the retention schedule. By erasing the information, or recording over it, the media is free for reuse.

1.6.6.3 Erasure of electronic media is considered destruction.

Approved by the County Commission October 6, 2022
Effective Date: November 1, 2022

_____	_____
Greg Mitchell, County Executive	Lana Jones, County Clerk