# JONES COUNTY

# ELECTRONIC MEDIA & TECHNOLOGY POLICY

*2/3/26*

## Table of Contents

**DEFINITIONS**

DEPARTMENT HEAD: As used in this policy, Department Head includes the Board of Supervisors, Elected Officials, appointed Department Heads and their designees.

ELECTRONIC MEDIA: Any form of media that uses electronic devices and technology to transmit, receive, view, or store information or content, including in the form of data, voice, or video.

IT DEPARTMENT: The IT Department refers to the County Information Technology Department.

IT COORDINATOR: The IT Coordinator refers to the IT Director or designee.

## ARTICLE 1 – USE OF ELECTRONIC MEDIA – GENERAL

The policies in this section apply to all use and access of County Electronic Media.

1.1 Authorized Use. Employees are responsible for safeguarding County information and assets by complying with this policy in their use of Electronic Media. Only employees or other users who are given authorized access may utilize County Electronic Media, including computers, email, telephone systems, servers, or databases. County provided Electronic Media are for County business use only, except where noted otherwise. The IT Coordinator, along with Department Heads, shall have collateral responsibility for administration of this policy.

This policy applies to all County employees and other authorized users of all types of County Electronic Media including, but not limited to, fax, Internet, Intranet, e-mail, messaging, social media, attachments, downloadable files, databases, and file systems *(network/local)*. *This* policy covers all types of County Electronic Media, including communications through the Internet and e-mail. The guidelines in this policy are not all-inclusive but are intended to illustrate both appropriate and inappropriate use.

Employees should not utilize County Electronic Media to say, do, write, view, or acquire anything that is not related to County business, is not related to their job-related responsibilities, and/or that are not appropriate for public disclosure. Each Department Head, in consultation with the IT Coordinator, is responsible for determining the types of Electronic Media, communications, or services which are required to fulfill an employee's job responsibilities. *No employee should consider their electronic communications (including social media usage) to be private when using County Electronic Media.*

Examples of appropriate uses of County Electronic Media include:

- Official intradepartmental communications with supervisors and other employees;
- Communications with members of professional organizations;
- Research of issues related to the County;
- Maintaining communication with supervisors and other employees when the employee is working off-site;
- Completion of reports and data entry;
- Retrieval of official reports;
- Performance of other tasks directly related to the employee's job description and assignment.

1.2 Unauthorized or prohibited use. County Electronic media may not be used to transmit, retrieve, and/or store any communication which:

- Discriminates or harasses (including but not limited to sexual advances, racial slurs, or other content which offensively addresses someone's age, sex, sexual orientation, religious or political beliefs, national origin, disability, or other protected class);
- Defames or threatens anyone;
- Contains obscene, profane, or pornographic material;
- Is used for any purpose which is illegal or infringes upon a copyright;
- Is inconsistent with County's personnel policies or work rules;
- Unduly interferes with the productivity of the employee or his/her co-workers;
- Consumes excessive system resources or storage capacity on an ongoing basis;
- Involves large file transfers or otherwise depletes system resources available for business purposes without permission of the IT Coordinator;
- Involves gambling or online game playing;
- Downloads or installs unofficial or unauthorized software from the internet, CDs, removable disks or drives, or any other source;
- Involves messages for personal gain, promotion, advertising or commerce;
- Operates a personal or freelance business or sells goods or services using County system(s) except by established procedures for use of the County Intranet system and devices;
- Attempts to remotely access any County system(s) using non-official means such as a backdoor or Trojan program or any other method in an attempt to circumvent the firewall and/or Internet monitoring software *(see management personnel exception in Section 1.3 of this addendum below)*;
- Sends or distributes any County licensed software or data unless specifically authorized to do so by the IT Coordinator;
- Gains unauthorized access (hacking) to remote or external systems *(see management personnel exception in Section 1.3 below)*.

1.3 Violations. Employees violating this policy are subject to discipline according to County policy, up to and including termination of employment. Any employee found to be deliberately accessing prohibited sites will have their access permissions immediately revoked.

The only exception is certain management personnel such as the IT Coordinator and the respective Department Head for the purposes of investigating policy infractions and/or testing of Internet monitoring software, as well as specifically assigned Law Enforcement Officers for official investigative assignments.

Employees using the County Electronic Media for defamatory, illegal, or fraudulent purposes may also be subject to civil liability and criminal prosecution.

Employees must immediately report to their Department Head any suspected violations of this policy. Department Heads must notify the IT Coordinator as soon as reasonably possible when the department head believes an employee has violated this policy.

1.4 Statutory Compliance and Confidentiality. County Electronic Media and technology must not be used to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way. Electronic communications containing protected health information may be subject to compliance with the County's Health Insurance Portability and Accountability Act (HIPAA) Policy. HIPAA Privacy and Security training shall be taken within the first 90 days of employment with the County as well as annually, if approved.

Employees working with County nonpublic, confidential, and/or protected information, including

confidential personally identifiable health, financial, personnel, or criminal justice information, must take all reasonable measures to safeguard such information, and shall not disclose such information to third parties, or save such information in unsecured, unauthorized locations outside County networks, without specific permission from the IT Coordinator or Department Head. Employees must follow appropriate Department procedures and encryption strategies to protect confidentiality.

1.5 Expectation of Privacy. County Electronic Media and output generated by, stored, or transmitted on such, as e-mail, messaging, word processing, utility programs, spreadsheets, voice mail, telephones, Internet/bulletin board system access, etc. are the sole property of County.

The County IT Coordinator may monitor usage patterns of any and all electronic media if requested by the respective Department Head. Elected Officials and/or Department Heads may, at their discretion, review an employee's electronic files, messages and usage to the extent necessary to ensure that County Electronic Media are being utilized in compliance with the law and County policies. Anyone accessing County Electronic Media, including employees, expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, the County may provide the evidence of such activity to law enforcement officials.

Electronic communications, including but not limited to e-mail and text messaging, utilizing County Electronic Media can constitute public records. It also may be accessed, produced, and used in a court of law for a lawsuit involving the County. The County is obligated to produce public records under Iowa Code Chapter 22, or when compelled by legal process. When under legal obligation, the IT Coordinator may review requests for access to the contents of electronic communication without the consent of a sender and/or recipient.

1.6 County Business Use. County Electronic Media are for use while conducting County business. Limited, occasional or incidental personal use of electronic media is understandable and acceptable subject to the discretion of the Department Head. Use of County Electronic Media for personal financial or commercial gain violates Iowa law.

1.7 County Image. Messages or information sent by an employee to one or more individuals via County Electronic Media can be statements identifiable and attributable to the County. All communications sent by employees via County Electronic Media must comply with this and other County policies and work rules and may not disclose any confidential or proprietary County information.

1.8 Security of System. County Electronic Media shall not be used in a manner that is likely to cause network congestion or significantly hamper the ability to access and use technology systems. Streaming video, music, or gaming websites is prohibited without prior approval from the Department Head.

Employee passwords to access County Electronic Media must be closely safeguarded and must not be provided to any outside or unauthorized user. All reasonable precautions must be taken to safeguard passwords and access codes; for instance, employees shall not leave passwords in plain view, or use non-secured or personal media to save or transmit their passwords. Passwords shall not be given to anyone except an employee's Department Head or IT Coordinator.

Forgery of email messages is prohibited. Attempts to read, delete, copy or modify e-mail of other users is prohibited *(see management personnel exception in Section 1.3 of this addendum)*.

Employees who are placed on a leave of absence, terminated or laid off from employment with the County have no right to the contents of their electronic messages and are not allowed access to

County Electronic Media. As stated elsewhere in this policy, employees should not be using County Electronic Media to send or store personal information. Management may access an employee's email, including if an employee is on vacation or other leave of absence.

1.9 Physical Security. Department Heads shall be responsible for all hardware assigned to their department. The IT Coordinator will secure all hardware not assigned to a particular department. All County Electronic Media will be stored in a secured location and/or locked environment. County data may not be removed from County premises without permission of the Department Head.

Employees are responsible for arranging their workstations in such a way so that the public and other employees without a need to know cannot casually see potentially confidential information on a workstation monitor. If this is not feasible, then privacy screen filters must be used on monitors.

Employees are required to notify the IT Coordinator if they believe it is not feasible to protect the confidentiality of what is visible on their monitors.

1.10 Network Security. The IT Coordinator shall assess risks to information from network, remote, and Internet connections and shall implement effective measures to protect the County's information. All users shall be granted their own user account on the County network upon receipt, by the IT Coordinator, of a written, or emailed, request from the Department Head (or designee). Users must select a secure password pursuant to the system's minimum requirements and shall not divulge that password to anyone, except on order of the employee's Department Head or of the IT Coordinator. The password must be changed as required by the County or relevant systems. Employees must be logged-out or otherwise secure their computers and other devices when the employee leaves their work location for the day.

1.11 Disaster Backup. The IT Coordinator shall maintain backups of all critical data on a scheduled basis.

1.12 **Work from Home/Remote Work Policy:**

At Jones County we believe in the value of working together in person to support collaboration, communication, and team culture. For that reason, employees are expected to perform their work on-site unless otherwise approved by the employee's Elected Official or Governing Board. No employee is entitled to, or guaranteed the opportunity to, work from home.

Working from home (also called "remote work" or "telework"), may be permitted **only in limited situations.** Approval will be based on employee job duties, performance, and business needs, or as required under applicable law.

When working from home:

- Work hours and schedules must remain the same as in-person office hours. Employees must be available and performing work during their regular work hours, and are expected to communicate regularly and effectively with managers and coworkers to the same degree that would be achieved if working on-site.
- All company policies on conduct, security, and attendance remain in effect.
- County systems and secure connections must be used for all work.
- Employees are responsible for maintaining a safe and ergonomic working environment while telecommuting.

IT Department must have written permission (Remote Access Request Form) from the Elected Official or Governing Board in order to set up the access.

Approval to work from home is a **privilege, not a standard practice**, and may be revoked at any time.

1.13Artificial Intelligence (AI) Proper Use:

Artificial Intelligence (AI) tools and platforms are increasingly prevalent and accessible. In the course of performing work for the County, generative AI may be used for secure, work-related purposes such as: drafting summaries, memos, or correspondence (subject to review); automating repetitive administrative tasks; organizing and analyzing data; creating presentation materials and content; and enhancing research processes.

However, the use of AI in the course of performing work is limited by the following tiers:

- Work product materials must be reviewed and validated for accuracy, and against any authoritative sources.
- All County policies and expectations on confidentiality, privacy, and data security apply. Employees may only use AI platforms which guarantee data isolation, encryption, and security, and employees must redact or de-identify any personal or confidential data before entering it into AI. Employees are strongly encouraged only to use AI platforms or add-ons specifically approved by their department.
- Employees are responsible for ensuring any work product or materials generated by AI are not violative of copyright or other intellectual property laws.
- The use of AI is subject to all County policies, including those pertaining to professional conduct and non-discrimination.

**Tier1 – Most employee – General Use**
**Permitted Tools:** Public facing, general available AI (e.g., ChatGPT, Co-Pilot, Gemini, etc.) or build-in AI features in software, used only for **NON-sensitive tasks**.
**Data Restrictions**: No personally identifiable information (PII), personal health information (PHI), Credit Card information (PCI-DSS) or confidential data may be input.
**Examples:** Brainstorming, summarizing public documents, drafting outlines, generating ideas.
**Guidance:**

- Employees may use these tools without special approval.
- Any output is reviewed by the user for accuracy before official use.
- Elected Officials/Department Heads reserve the right to limit or revoke AI usage at their discretion.

**Tier 2: Moderate/High-Risk / County-Licensed Use**
**Permitted Tools:** AI services with additional data handling or enterprise security assurances (e.g., Microsoft 365 CoPilot – **under county license**, (contact IT if you need this access for a license.)
**Data Restrictions**: May involve regulated or highly sensitive data, (e.g., PHI, law enforcement data). Deidentified, fictitious or encrypted data is strongly recommended.
**Examples:** Sheriff's office analyzing law-enforcement data (CJIS). Public Health Department using PHI for analytics under HIPAA-complaint cloud infrastructure. Drafting certain internal documents, preliminary analysis involving limited or deidentified data.
**Guidance:**

- Requires an approved request to the IT Department and use of licensed accounts (no free trial or personal accounts)
- Departments may be required to demonstrate intended use, benefits, and alignment with policy.
- Any moderate-risk AI usage must still comply with HIPAA, CJIS, PCI-DSS or other relevant

regulations.

Any violations of this policy can result in discipline, up to and including termination.

## ARTICLE 2 – INTERNET USAGE

2.1 Confidentiality. Communications and information transmitted over the Internet should be treated as non-confidential. Anything sent through the Internet passes through a number of different computer systems, all with different levels of security. The confidentiality of messages may be compromised at any point along the way.

2.2 Security. Under no circumstances shall County information of a nonpublic, confidential, sensitive or otherwise proprietary nature be posted online, including an employee's social media. (See Social Media Policy, Article 5). County information posted on the Internet must reflect the standards and policies of County.

2.3 Unauthorized Access. Unless the prior approval of IT Coordinator has been obtained, users may not establish Internet or other external network connections that could allow unauthorized persons to gain access to County's systems and information. These connections include but are not limited to the establishment of hosts with public modem dial-ins, World Wide Web (WWW) home pages, File Transfer Protocols (FTP), File Sharing Sites, (Dropbox, Google drive, One Drive, and similar), sites that allow County owned computers to be accessed remotely, and non-County authorized wireless or wired access points.

2.4 Viruses. All file downloads from the Internet must be checked for possible viruses. If uncertain whether your virus-checking software is current, you must check with the IT Coordinator before downloading any file or e-mail attachment.

2.5 Loss Resulting from Personal Use. The County accepts no responsibility for any loss incurred to an employee for any personal use of the County Internet and e-mail services including, but not limited to, technical problems with any County security system(s) or access to employee personal or financial data transmitted or stored through County systems.

2.6 Outside Entities and Internet Usage. Outside Entities may request use of County Network resources, including the Internet, when onsite and/or working with the County, and the IT Coordinator should be contacted. The IT Coordinator may review any and all equipment, peripherals, drives, etc. to be used by the outside entity that will or could have direct or indirect contact with the County network. This policy supersedes any and all policies of an outside entity pertaining to the equipment that is attached to the County network. The outside entity must comply with the terms of this policy and any requests of the IT Coordinator.

2.7 Public/Outside Wifi. County employees are prohibited from connecting County devices to public Wifi networks for cybersecurity reasons. If a County employee or elected official needs to access the Internet for County business while outside of the County, they should contact the IT Director for a hotspot connection.

## ARTICLE 3 – EMAIL

The electronic mail (e-mail) system hardware and software is the property of the County. All messages composed, sent, or received on the email system are the property of the County.

3.1 Email Audits. The County reserves and intends to exercise the right to review, audit, intercept, access, and disclose all messages created, received, or sent over the County email system for any purpose. E-mail may be audited by designated persons to ensure compliance with this policy. County employees have no expectation of privacy in any emails, attachments, or content sent through County emails accounts or through County Electronic Media.

3.2 E-mailing Large Files. Exercise caution when transferring "large" files. If an employee is unsure about the current definition for a "large" file, they should contact the IT Coordinator about how best to handle "large" file transfers.

3.3 News Groups and Mailing Lists. Subscriptions to news groups and mailing lists on County email are permitted when the subscription is for a work-related purpose. Any other subscriptions are prohibited.

3.4 Managing E-mail Account. Employees are responsible for managing their e-mail, Sent Items, and Deleted Items folders. It is recommended to check for new messages at least once per workday.

3.5 Remote Access of E-mail. Transferring County information to a home computer and/or any other personal electronic device is prohibited whether in the form of e-mail, file attachment, or wireless transmission unless approved by your Department Head. The County does provide for the use of remote access methods, including remote e-mail access, to County files outside of the office environment. The proper method of transferring the files is e-mail unless another mechanism is specifically approved by the IT Coordinator. Please consult with the IT Coordinator as to the best method to use. Note: Employees who are not exempt under the Fair Labor Standards Act (FLSA) are not allowed to check e-mail remotely without prior approval of their Department Head. (See Work From Home/ Remote Access Policy – Section 1.12).

3.6 E-mail Backup and Retention. E-mail messages, including County email, and other email services including gmail, yahoo, and exchange accounts accessed on County computers, are stored by the County for a predetermined time as established by the IT Coordinator as part of normal backup procedures. This predetermined time may change periodically, as necessary, in the normal course of operations. It should be noted that even though an e-mail message is marked "Deleted" by the user, it may still be stored through the County's normal electronic backup procedures.

3.7 Personal E-mail Accounts. Accessing or "checking" of personal e-mail on county computers is strictly prohibited. This includes web-based services such as Yahoo, MSN, Gmail, and any similar services, unless specifically authorized by the employee's Department Head.

## ARTICLE 4 – NETWORK FILES SYSTEM/PERSONAL COMPUTERS/ELECTRONIC DEVICES/PERIPHERALS

4.1 Software Licensing Agreements. The County maintains, and will enforce strict adherence to, software vendor's licensing agreements. When using County computing and/or network resources, copying of software in a manner which violates the vendor's license agreement is prohibited. Participation, including during off-duty hours, in the use or distribution of pirated software or content is prohibited. Reproductions of words or images posted or otherwise available over the Internet must be done only with the permission of the author/owner.

4.2 County's Right to Examine Stored Information. The County reserves the right to examine e-mail, directories and files and any information stored on any County computer, flash drives, cloud storage, or other electronic media at any time and without prior notice. Examination will be done to assure compliance with County internal policies, support the performance of internal investigations, and assist with the management of County information systems.

4.3 Authorized Downloads. County employees may download only work-related files to the County network or to their local hard drive, flash drives, or other electronic media devices. All such files must be scanned for viruses prior to use.

4.4 Resale or Transfer of Information Prohibited. Any County owned or licensed software, hardware, or files must not be sold or otherwise transferred to any non-County party for any reason other than business purposes expressly authorized by the Board of Supervisors.

4.5 Firewall System. A "firewall" device is installed at the Internet gateway connection point to control access to/from the County network. This connection into the Internet is the only authorized link between the Internet and the County network. The use of proxies to disguise Internet activity is prohibited. No attempt should be made to bypass the County firewall system to obtain Internet access.

4.6 Temporary Internet Files. No attempts shall be made to hide/encrypt any temporary Internet files unless approved by the IT Coordinator. Default (supplied) settings pertaining to temporary internet files; cookies, etc. are not to be altered.

4.7 Purchase and Installation. Only County-purchased hardware/software is allowed to be connected/installed to County-owned computer equipment and/or the County network.

Department Heads are encouraged to communicate with the IT Coordinator prior to purchasing a technology-related product to ensure the product is compatible with the County's network and IT capabilities. The IT Coordinator will research products, price compare, and provide recommendations to Department Heads at the Department Head's request. All electronic hardware, wired, wireless, mobile or peripherals that are connected to the County network must be installed and attached by the IT Coordinator.

All defaults set by the IT Coordinator shall be left as set when installed. Any attempts to change these defaults may be considered a violation of computer security under Sections 1.1, 1.2, and 1.3.

4.8 Connections. Connection of any wireless access point or hub/switch to the County network is prohibited unless approved by the IT Coordinator and installed by the IT Coordinator or designee.

4.9 Use of Another's Network Password Prohibited. Employees should never use another employee's password to access a file or retrieve any stored communication unless specifically authorized to do so either by the IT Coordinator and/or the Department Head for purposes of business continuity. Network passwords are to be kept in confidence and not to be divulged to any third party unless specific authorization is given by the IT Coordinator to release a password for purposes of vendor support.

## ARTICLE 5 – SOCIAL MEDIA POLICY

5.1 Purpose. The purpose of this policy is to establish guidelines for the use of social media by employees of County, while at and off work. It is impossible to anticipate or address all aspects of social media within a policy; however, this policy should be used as a guide. The Board of Supervisors, elected officials and department heads reserve the right to interpret this policy and apply it on a case-by-case basis within their respective departments.

5.2 Personal Use of Social Media. The County acknowledges employee rights to free speech that may protect online activity conducted on personal social networks. However, what is published on such personal sites should not be attributed to the County and should not appear to be endorsed by or originated from the County. Make it clear that your views do not represent those of your department, your Department Head, or the County. Employees that choose to list their work affiliation or reference their employment with the County in any way on a social network should understand it may be subject to review by the County.

5.2.1 Even personal social media use may result in discipline, up to and including termination, if it adversely affects your job performance, the job, performance of co-workers, or otherwise causes substantial disruption to the workplace and/or County operations. Employees assume all risk associated with their off-duty personal use of social media.

5.2.2 Employees are prohibited from accessing social media for personal use while on work time. Employees are also prohibited from using County Electronic Media to access social media unless approved or directed by their Department Head.

5.2.3 Employees who choose to engage in personal social media on their own time and equipment may not:

- Attribute personal statements, opinions, or beliefs to the County; or
- Disclose nonpublic, confidential, proprietary, or sensitive County information, including but not limited to personally identifiable information about co-workers, supervisory staff, clients, customers, patients, applicants for permits, inmates, persons taken into custody, calls for service, employee disciplinary actions, and other such matters; or
- Use County logos or trademarks; or
- Post any material that constitutes hate speech, libel, or defamatory comments; creates a hostile or intimidating work environment under the harassment policies of the County; or threatens/incites violence.

5.2.4 Violations of this policy may result in disciplinary action as provided for in the County Employee Handbook including, but not limited to, termination of employment.

5.3 County Endorsed/Approved Use of Social Media for Departmental Use. Certain types of social media may be approved by the Board of Supervisors or a Department Head to promote the programs and activities of the department, or as a means to disseminate information to the public.

5.3.1 The Department Head and/or IT Coordinator shall determine the types of social media that will be used, the content to be included in approved sites and feeds and designate the employee(s) responsible for posting to approved social media sites and feeds. The IT

Coordinator and/or respective Department Head (or designee) will create and maintain all County endorsed social media sites. All changes, posts or updates must be made by IT personnel or the Department Head (or designee).

5.3.2 A department with a social media site or feed is responsible for monitoring the content on those sites and feeds, establishing rules and guidelines for public use, and monitoring use. The Department Head will be responsible for notifying the public and/or issuing press releases if the site or feed is compromised. The IT Coordinator must also be notified if any inappropriate activity is found, as network security may be at risk.

# COUNTY ELECTRONIC MEDIA & TECHNOLOGY POLICY

## ACKNOWLEDGEMENT & AUTHORIZATION

I hereby acknowledge that I have received a copy of the Jones County Electronic Media & Technology Policy. I understand that the County has the right to monitor its systems and networks, including periodic review of the computer system. I understand that all Internet use, email communication, and all information transmitted by, received from, or stored in these systems are the property of County. I have no expectation of privacy in connection with the use of County Electronic Media or with the transmission, receipt, or storage of information in or through this media. I shall take all measures to protect the confidentiality of County information and security of its systems, as set forth in this policy.

I acknowledge and consent to the County monitoring my Electronic Media, Internet, Email, Social Media, and AI use at any time as provided by this Policy. I understand that this Policy shall not be construed to be a contract and may be modified by the County Board of Supervisors at any time.

**I have read all of the provisions specified in this policy.**

_____ _____

Employee Signature Date

_____

Job Title

*[Printed Employee Name]*

_____ _____

First Last

_____ _____

Department Head Date

4922-5717-5686-1\22987-001

# Remote Access REQUEST FORM

## Employee Info

Name: _____ Date: _____

## Computer Info

**Office Desktop Name:**

_____

## Remote Access

**Do you need remote access indefinitely?**

☐ Yes ☐ No

**If no, what days do you need remote access?**

From: _____ Until: _____

## Employee Signature:

I have read and will follow the Work from Home/Remote Work Policy and acknowledge that I must have the an MFA authentication app on my mobile device for remote access.

**Signature:** _____ **Date:** _____

## Elected Official Signature:

**Signature:** _____ **Date:** _____

## For IT Use

Date Request Received:

_____

Date Remote Access Granted:

_____

Date Remote Access Removed (if applicable):

_____