Benton County
Acceptable Usage
Policy

September
12, 2017

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 electronic device designed to transmit, receive, or store information in the form of data, voice, video, or Internet.

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

1.1 Authorized Use. Employees are responsible for safeguarding County information and assets by complying with this policy. Only employees or other users who are given authorized access may utilize computerized electronic communications. Electronic communications are for County business use only, except where noted otherwise.

Employees should not say, do, write, view, copy, transmit or acquire anything that would not be considered to be County Business; that does not require access to job related responsibilities; and/or would be contrary to law or inappropriate under the terms of this policy. Each Department Head, in consultation with the IT Coordinator, is responsible for determining the types of electronic communication or services which are required to fulfill an employee's job responsibilities. The IT Coordinator, along with Department Heads, shall have responsibility for administration of this policy. This policy applies to all County employees and other authorized users of all types of electronic communications including, but not limited to, fax, Internet, Intranet, e-mail, messaging, attachments, downloadable files, and file systems (network/local). No employee has any expectation of privacy in any communications made over County-owned information technology systems or equipment. This policy covers all types of electronic communications with emphasis on the Internet and e-mail. These guidelines are not all-inclusive but are intended to illustrate both appropriate and inappropriate use except where provided in this policy.

Examples of appropriate uses of these resources 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. Electronic media may not be used to transmit, retrieve, and/or store any communication which:

Discriminates or harasses (including but not limited to race, religion, color, sex, age, national orgin,sexual orientation, gender identity, disability or any other characteristic protected by local, state or federal law);

Defames, threatens, or derides (i.e., contain derogatory comments toward or about) any individual group or protected class;
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;
Involves any prohibited activity;
Interferes with the productivity of the employee or his/her co-workers;
Consumes 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 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;
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
Sends or distributes any County licensed software or data unless specifically authorized to do so by the IT Coordinator;
Uses the County's electronic media to gain unauthorized access (hacking) to remote or external systems.

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 connection immediately revoked (with the exception of 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). This policy excludes any bona fide law enforcement intelligence gathering as defined in the Iowa Code. Employees using the County computer system 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 Expectation of Privacy. Electronic media and output generated by such, and/or communicated by an employee using 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 will 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 electronic media and services are being utilized in compliance with the law and County policies. Anyone accessing this system 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 can be used during discovery in a court of law. The County will disclose any such communications to law enforcement officials or others so authorized by a court of law if legally required or pursuant to legal process as defined in the Iowa Code. When under legal obligation, the IT Coordinator will review requests for access to the contents of electronic communication without the consent of a sender and/or recipient.

1.5 County Business Use. Electronic media and services 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. Commercial or partisan political use is a violation of Iowa Code Section 721.2.

1.6 County Image. Messages or information sent by an employee to one or more individuals via electronic media are statements identifiable and attributable to the County. All communications sent by employees via electronic media must comply with the Acceptable Usage Policy and other County policies and work rules and may not disclose any confidential or proprietary County information.

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

Passwords shall not be given to anyone except an employee's Department Head or IT Coordinator at the Department Head's request. Holders of mailboxes are accountable for all messages sent from their e-mail account, unless it is established that another person sent a message from the holder's e-mail account.

Forgery of electronic mail messages is prohibited. Unless otherwise provided by this policy or by permission of the user, 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 the electronic communication system. Management may access an employee's electronic mail at any time necessary for County business purposes or the enforcement of this policy.

1.8 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 electronic media will be stored in a secured location and/or locked environment. 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.

1.9 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 in 90-day intervals. Employees must be logged-out or otherwise secure their computers and other devices when the employee leaves their work location for the day.

1.10 Disaster Backup. The IT Coordinator shall, at a minimum, maintain daily backups of all critical data.

ARTICLE 2 – INTERNET USAGE

2.1 Confidentiality. Internet messages 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. Employees working with protected information, including confidential health information or criminal justice information, must follow appropriate department procedures and encryption strategies to protect confidential documents.

2.2 Security. Under no circumstances shall information of a confidential, sensitive or otherwise proprietary nature be placed on the Internet. Because postings placed on the Internet may display the employer's address, information posted on the Internet must reflect the standards and policies of County.

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

2.4 Copyrighted Material. Information posted or viewed on the Internet may constitute published material. Therefore, reproduction of information posted or otherwise available over the Internet may be done only with express permission from the author or copyright holder.

2.5 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, and similar), sites that allow County owned computers to be accessed remotely, and non-County authorized wireless or wired access points.

2.6 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.

2.7 Inappropriate Use. Offensive, demeaning or disruptive messages are prohibited. This includes, but is not limited to, messages or links to websites that are inconsistent with the County's policies concerning "Equal Employment Opportunity, Harassment, and ADA Compliance" and "Preventing Sexual Harassment in the Workplace." The County uses independently supplied software and data to identify inappropriate or sexually explicit Internet sites. Access from within the County network to all such sites may be blocked by the IT Coordinator. If an employee accidentally connects to a site that contains sexually explicit or offensive material, they must disconnect from

that site immediately. Any employee found accessing prohibited sites in violation of this policy could have their connection revoked (see management personnel exception in Section 1.3). Sexually explicit material includes any depiction of male or female nudity or partial nudity, or sexual activity, any offensive textual or verbal reference (voice recording) to sexual activity or nudity including jokes, stories, reports, blogs or any other material with content which could be construed as offensive or adult in nature.

2.8 Display of Explicit Image or Document. The display of any kind of sexually explicit image or document on any County system is a violation of the County's Workplace Harassment policy. Sexually explicit material may not be archived, stored, distributed, edited or recorded using the County network or any County computing resources.

2.9 Statutory Compliance Required. County Internet services and computing resources must not be used to violate the laws and regulations of the United States, or any state, city, or other local jurisdiction in any material way. Electronic communications containing protected health information are 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. Use of any County resources for illegal activity is subject to disciplinary action in accordance with County policies.

2.10 Self-Identification. Each employee using the Internet services of the County shall identify himself or herself honestly, accurately and completely (including one's County affiliation and function where requested) when participating in chats or newsgroups on County time, or when setting up accounts that discuss County business on outside computer systems.

2.11 Safe-guarding Information. County credit card numbers, telephone calling card numbers, log-in passwords and other parameters which can be used to gain access to goods or services, must not be sent over the Internet in readable form. The County will not be held responsible for the security and use of personal credit card numbers, telephone calling card numbers, or other personal information sent via the Internet for business purposes.

2.12 Loss Resulting from Personal Use. The County accepts no responsibility for any loss incurred in relation to personal use of the County Internet and e-mail services including, but not limited to, technical problems with any County security system(s).

2.13 Certain Uses Prohibited. Installation and usage of instant messaging or chat programs/services or real-time messaging collaboration, online dating/friend finder services, real-time weather or time programs (unless specific for business needs as determined by the Department Head and the IT Coordinator) are prohibited.

2.14 Outside Entities and Network Usage. Outside Entities may request use of County Network resources, printers, etc. The IT Coordinator maintains a limited but free Wi-Fi connection for outside entities while visiting the county buildings. If the free Wi-Fi does not meet the needs of the outside entity then they may request to use the County's network resources. To obtain access to the County network, the entity must submit a written request to the IT Coordinator. Upon approval by the IT Coordinator, the entity must complete and return the last page of the current Electronic Media and Technology Policy Addendum which will be kept on file with the IT Coordinator's office. The entity will be bound by the current IT policy. 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. The County's policy takes precedence over any policies of an Outside Entity that pertain to any equipment included in the County network and an Outside Entity must comply with the terms of this policy and any requests made by the County's IT Coordinator.

ARTICLE 3 – ELECTRONIC MAIL

The electronic mail (e-mail) system hardware and software is the property of the County. All messages composed, sent, or received on the electronic mail system are the property of the County and are not the private property of any employee.

3.1 Access without Permission. Except for the IT Coordinator and/or Department Head, employees shall not attempt to gain access to another employee's messages without the employee's permission (see management personnel exception in Section 1.3 of this addendum).

3.2 E-mail Gateway. E-mail allows Internet mail to be sent and received via the County network. The IT Coordinator will maintain the e-mail gateway. There will be only one gateway in order to provide a common address naming structure for Internet users accessing e-mail through the County's network. Attachments to e-mail are allowed up to a file size as specified by the IT Coordinator. The e-mail gateway and the Internet gateway connection point are the responsibility of the IT Coordinator. All employees must remember that data sent via the Internet could potentially be intercepted and read or subject to disclosure under Iowa's open records laws. It is essential that all data transmitted via e-mail through the Internet, as well as within the County, be of an appropriate nature. Employees will be accountable for the content of sent and retained e-mails.

3.3 Use of E-mail. The County's e-mail system is intended for official business usage only. Incidental usage that does not violate any of the other terms in this policy may be permitted on an occasional basis. All business or personal incidental usage is considered public information and subject to disclosure at any time.

3.4 Prohibited Messages. Offensive, demeaning or disruptive messages are prohibited. This includes, but is not limited to, messages that are inconsistent with County's Equal Opportunity and Workplace Harassment Policies.

3.5 E-mail 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 electronic mail system for any purpose. E-mail may be audited by designated persons to ensure compliance with this policy. The contents of electronic mail properly obtained for legitimate business purposes may be disclosed without the permission of the employee.

3.6 Confidentiality. The confidentiality of any message cannot be assured. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality. Electronic communications containing protected health information are subject to compliance with the County's Health Insurance Portability and Accountability Act (HIPAA) Policy. Messages containing protected health information or other confidential data or information should be encrypted. Contact the IT Coordinator for the current procedure for sending encrypted messages.

3.7 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.

3.8 Managing E-mail Account. Employees are responsible for managing their e-mail, Sent Items, and Deleted Items folders. It is required to check for new messages at least once per workday. Employees are recommended to set an out of office with department contact information.

3.9 Sending/Receipt of Unacceptable E-mails. The sending of chain letters, games and jokes, bulk mailings, and display of personal advertisements or solicitations over the County network is not permitted. Sending abusive or threatening e-mails or obscene or pornographic attachments is not

permitted. If an employee receives any of these types of e-mails, they should delete them immediately and not forward them to any other recipient. They should also notify any sender of these types of e-mails to cease and they should keep a record of such notice in case any discrepancies arise in the future. If messages do not cease or the employee cannot cease the messages after reasonable action taken on their part, the IT Coordinator should be contacted for assistance.

3.10 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 access 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.

3.11 Remote Access of County Network. In order to maintain network security and integrity, access is limited and strict security protocols will be implemented for employees that require access. Employees not exempt under the FLSA will not be allowed to access the County network remotely. The IT Coordinator will establish and maintain the necessary security procedures and policies needed to maintain a secure environment at the County. Employees must adhere to these policies and procedures.

3.12 E-mail Backup and Retention. E-mail messages (both 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.

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-hours) in the use or distribution of pirated software, bulletin boards and similar activities 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, tapes, disks, 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 network or to their local hard drive, floppy 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. County software, documentation and all other types of information must not be sold or otherwise transferred to any non-County party for any purposes other than business purposes expressly authorized by the Board of Supervisors after consultation with the IT Coordinator.

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 unless written approval is obtained from the IT Coordinator (see management personnel exception in Section 1.3).

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. “Private” browsing sessions are prohibited.

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. Personal devices will be allowed with the discretion of the IT Coordinator with approval by Department Head

Department Heads are required to obtain permission from 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.

All electronic hardware, wired, wireless, mobile or peripherals that are connected to the network must be purchased, installed and attached by the IT Coordinator with written authorization by the Department Head (or designee) of the department where it will be used.

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 network is prohibited unless approved by the IT Coordinator and installed by the IT Coordinator or designee.

4.9 Use of Another ’s 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. At the request of the Department Head, an employee must provide the County with a sealed hard copy record of all passwords and encryption keys for County use.

4.10 Prohibited Actions. Employees may not attempt to read or “hack” into other employees’ assigned computer/e-mail, crack passwords, breach any computer or network security systems, or intercept any electronic communications not intended for the employee (see management personnel exception in Section 1.3).

4.11 Mobile Devices.

Mobile Devices, including but not limited to: laptops, cell / smart phones, iPads, etc. that are issued by the county as well as personal devices (limited to cell phones / smart phones only) that are used for business purposes and / or store county information shall adhere to the following guidelines:

Access to County information resources using a mobile device must be pre-approved by the IT Administrator and the Department Head / Elected Official;

Mobile devices must require a pin / pattern / password lock to access; Mobile devices must require a pin / pattern / password lock after a period of inactivity;

Encryption is required for all mobile devices that must store or access sensitive information. (Please contact the IT Administrator for assistance establishing data encryption);

Users that use personal mobile devices for business must follow the same guidelines as those users who are issued County-owned devices;

Users will physically secure mobile devices that are left unattended. (If left in a vehicle, mobile devices will be hidden from view, locked in glove compartment, etc.);

Users are not allowed to provide unattended access to mobile devices by another user;

Users will notify the IT Administrator immediately if mobile device is lost or stolen;

Users will return County provided mobile devices at the end of employment. At which time the device will be wiped after it is checked for status of County-related information on the device.

Personal devices, excluding cell phones / smart phones, shall not be connected to any County network.

County owned devices will also be required to have a MDM (mobile device management) application installed on the device to allow remote monitoring of the device and will allow the IT Department to remotely wipe the device if lost or stolen. The auditor's office will have access and authority to any departments cell plans to audit usage and plan details.

4.12 Training.

The IT Administrator shall establish periodic End User Security Training. All End Users of County Systems shall be required to attend this training and / or review the training materials provided during the training session. Each training session shall include an End User Acknowledgement Sheet to be signed and dated by the End User.

ARTICLE 5 – SOCIAL MEDIA POLICY

5.1 Purpose. The purpose of this policy is to establish guidelines for the use of social media and downloadable applications by employees of County, while at and off of work. It is impossible to anticipate or address all aspects of social media within a policy; however, this policy should be used as a guideline. 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 privacy and free speech, including the right to comment on matters of public concern, that may protect online activity conducted on personal social networks or other electronic forums. Such rights are not, however, without limits, and conduct or statements that interfence with the functioning of the workplace are subject to evaluation by the county. 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. An employee should 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 regard all communication on that network as if it were a professional network, and subject to review by the County.

5.2.1 County employees engaging in social media networks must at all times be conscious and respectful of the fact that their words and actions may be taken as being representative of the County, regardless of when, where and how the content is posted. Any conduct that adversely affects your job performance or the performance of co-workers or otherwise adversely affects employees, supervisory staff, users of the services or the legitimate business interests of a department or the County may result in disciplinary action up to and including termination of employment.

5.2.2 Employees assume all risk associated with their off-duty personal blogging and use of social media. The County may require immediate removal of material and/or take disciplinary action for personal blogging or personal use of social media by employees that causes a disruption of the workplace or impairs the statutory and/or implied duties and responsibilities of the County.

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

5.2.4 Employees who choose to engage in personal online blogging or social media on their own time and equipment may not:

Attribute personal statements, opinions, or beliefs to the County; or

Disclose confidential 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 similar matters; or

Use County logos or trademarks; or

Post any material that constitutes; violates the privacy rights of fellow employees; is disruptive to the work environment by impairing discipline or control; interferes with job performance; creates a hostile or intimidating work environment under the harassment policies of the County; or obstructs operations; or Post photos, video, or audio taken inside or outside any county owned property without permission of the Department Head, or their designee(s).

5.2.5 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 IT Coordinator shall determine the types of social media that will be used, the content to be included on approved sites and feeds and designate the employee(s) responsible for posting to approved social media sites and feeds. The IT Coordinator or Department Head (or designee) will create and maintain all County endorsed social media sites. All changes, posts or updates must be done by IT Coordinator 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 for inappropriate posts. The IT Coordinator and 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. The IT Coordinator reserves the right to remove any/all information off of a county social media site if it is determined that it does not meet County Social Media standards

BENTON COUNTY ACCEPTABLE USAGE POLICY

ACKNOWLEDGEMENT & AUTHORIZATION

I hereby acknowledge that I have received a copy of the Benton County Electronic Media & Technology Policy. I understand that the county has the right to monitor the system for illegal or unauthorized activity, including periodic review of the computer system. I understand that all Internet, email communication systems 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 this equipment or with the transmission, receipt or storage of information in this equipment. I agree to not use a code, access a file or retrieve any stored communication unless authorized. I acknowledge and consent to the county monitoring my 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