Dubuque County Administrative Policy

Subject: Use of County Technology
Effective Date: October 14, 2019

General 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, applications, and file systems.

Scope:

This policy is applicable to the following:

All employees responsible to the Dubuque County Board of Supervisors;

All employees responsible to a County elected office holder providing the appropriate elected office holder and the Board of Supervisors have certified its applicability;

All employees not directly responsible to either the Board of Supervisors or an elected office holder and whose governing body and the Board of Supervisors have certified its applicability.

Provisions:

Use of Electronic Communications – General

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. Upon notification of the new employee from the Human Resources (HR) Department, the Information Technology (I.T.) Department will work with each Department Head or elected official to determine the types of electronic communication or services which are required to fulfill an employee's job responsibilities.

   Employees are responsible for the proper use and care of all County equipment including computers, smartphones, cell phones and tablets issued to them and must ensure that the technology is stored in a secured manner. Employees are required to immediately report any theft of County-issued equipment to their department Elected Official or Department Head.

2. Unauthorized or prohibited use
   Electronic communication may not be used to knowingly view, transmit, retrieve, or store any communication which:

- Discriminates or harasses (including but not limited to sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin, or disability);
- Defames or threatens any individual group or protected class;
- Contains obscene, profane or X-rated material;
- Is used for any purpose which is illegal or infringes upon a copyright;
- Is inconsistent with County 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;
- Involves gambling or online game playing;
- Involves couponing or online deals schemes;
- 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 sell goods or services using County system(s);
- 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 security monitoring software;
- Sends or distributes any County licensed software or data unless specifically authorized to do so by the I.T. Department;
- Sexually explicit material may not be archived, stored, distributed, edited or recorded using the County network or any County computing resources.

3. <u>Expectation of Privacy and Monitoring</u>

Electronic communications and output generated by such, and/or communicated by an employee using e-mail, messaging, word processing, spreadsheets, voice mail, telephones, Internet, etc. are the sole property of County and are public records unless otherwise provided by the Iowa Open Records Act (Chapter 22). Users should exercise care regarding the content of their transmissions.

The County maintains the right and ability, with or without notice to the employee, to access and review any information contained on County technology, even if protected by private password. Those individuals using County technology have no expectation of privacy in connection with the use of such technology or transmission, receipt, or

storage of information through the use of such technology. Anyone accessing the system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, County may provide the evidence of such activity to law enforcement officials.

Elected Officials and Department Heads may review an employee's electronic files and all communications to ensure compliance with the law and County policies. In order to ensure transparency, the request for this information will be facilitated by Human Resources.

In the event of a time sensitive matter in which a Department Head or Elected Official needs to access an employee's local computer or network shares for work related reasons, the IT Department will assist them and not require the involvement of Human Resources.

4. County Business Use

Electronic communications and services are for use while conducting County business only. Limited, occasional, or incidental personal use of electronic communication is understandable and acceptable subject to the discretion of the Elected Official or Department Head. Such personal use is permitted provided (1) it does not interfere with the performance of the employee's job duties and obligations; and (2) it does not violate this policy or any other County policy; and (3) it does not interfere with the operation of County technology.

An employee's County e-mail address should not be used as or considered to be a personal e-mail address and must not be used as such.

5. Security of System

Electronic communication 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.

Passwords shall not be shared with others or left in plain sight. Passwords should only be shared with the IT Department if they are actively helping you troubleshoot some technology related issue. No other employee including a Department Head or Elected Official should have access to your password except in extenuating circumstances and after that circumstance has passed, the employee should change their password.

Employees are responsible for selecting a challenging password and are encouraged to think of a passphrase vs. password.

Password example: iowacorn720
Passphrase example: I love Iowa Corn!

The password requirements may change as new best practices are implemented at the County and employees should contact the helpdesk if they need guidance on creating a strong password that matches current industry standards.

Internet Usage

6. 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.

7. Viruses
   All file downloads from the Internet are automatically checked for possible viruses. If you receive a suspect file contact the IT Department for guidance before opening said file.

8. Inappropriate Use
   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 I.T Department. If an employee accidentally connects to a site that contains sexually explicit, offensive, or inappropriate material, they must disconnect from that site immediately.

   County Internet services 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 are subject to compliance with the County's Health Insurance Portability and Accountability Act (HIPAA) Policy.

   County purchasing 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 or other personal information sent via the Internet for business or personal purposes.
   Installation of any software that is not part of the standard County computer setup must be approved by the IT Department. This includes communication software that while may be meant to be used for business reasons, must still be approved before install and use.

Electronic Mail

The electronic 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.

9. Access

Except for the Elected Official, Department Head, or authorized I.T. staff, employees shall not attempt to gain access to another employee's messages without the employee's permission.

10. County Business Use

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.

All employees must remember that data sent via the Internet which is a public transport system could potentially be intercepted and read. 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 should be aware that e-mail is not a completely secured method of communicating and is possible to be intercepted by a third party.

E-mail supports attachments and the number and total size may change as technology evolves. Employees should contact the IT Department for current restrictions.

Employees have the ability to send a higher level of secured e-mail message if such a unique situation is required and should contact the IT Department for guidance.

The employee signature line at the bottom of every e-mail message shall include the user's name, title, department and telephone number. The signature line may include the County webpage, employee fax number, or social media links. The signature line is to remain professional and not include superfluous items.

11. Inappropriate Use

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.

12. Remote Network Access by County Employee or Support Vendor

Remote network access to County systems is available for employees who require access after-hours and for extenuating circumstances.

Employees should contact their supervisor for permission and if granted, IT will work to implement the access in conjunction with the wishes of the Department Head or Elected Official. Remote access can take different forms but VPN is a common term for it.

County files and information must not be stored on personal devices. Downloading or copying files from the County network to a personal device when doing remote network access is prohibited.

Authorized vendors may need to remotely access the County network for support reasons. Any County employee giving access to a vendor for support reasons is responsible for the actions that vendor may take if those actions are malicious.

13. E-Mail Access

E-Mail access is available via Web Interface and personal devices however the IT Department may restrict employees for security reasons or if requested by the supervisor of the employee.

If you use County e-mail on a personal device, downloading attachments to your personal device should be avoided.

An employee that is classified as exempt pursuant to the Fair Labor Standards Act may access a County account from a remote location other than the site designated for that account (e.g., telecommuting or checking e-mail while away from the office on business) only with approval of the employee's Department Head or Elected Official and only for County business.

As with other types of authorized work, all time spent by non-exempt (hourly) employees using electronic communications or services for work purposes will be considered hours worked; the time is compensable and will count toward overtime eligibility as required by law.

Non-exempt employees should not check for, read, send, or respond to work-related e-mails outside their regularly scheduled work hours unless pre-authorized by their Department Head or Elected Official to do so. Non-exempt employees using cellular or smartphones for work-related correspondence during unauthorized times may be subject to discipline for violating this policy.

14. Record Retention

The I.T. Department will maintain a copy of all emails sent or received for a period of seven (7) years from the date in which they are sent or received. Records may be retained for a longer time period if it is subject to a litigation hold. 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.

The County differentiates between the live email mailbox of an employee and the archived email mailbox that is used for litigation purposes.

The employee is free to manage their live inbox as they deem most beneficial to their work style and e-mails will not be forcibly deleted from this inbox.

The archived e-mail mailbox is considered the county record for email and will be automatically purged at midnight every day for all e-mails over seven years.

Network File System

15. Monitoring, Access and Usage

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.

The County maintains, and will enforce strict adherence to, software vendor's licensing agreements. When at work or when using County computing and/or network resources, copying of software in a manner which violates the vendor's license agreement is prohibited.

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. A small amount of personal pictures are exempt from the download only requirement above provided they do not cause any technology related problems with the computer and are compliant with all County policies.

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 Board of Supervisors.

The use of proxies to disguise Internet activity is prohibited. No attempt should be made to bypass the County security systems to obtain Internet access unless approved by the I.T. Director.

No attempts shall be made to hide/encrypt any temporary Internet files unless approved by the I.T Director. Default (supplied) settings pertaining to temporary internet files, cookies, etc. are not to be altered. Using a web browser's private or equivalent mode is prohibited.

No personally owned device/peripheral/electronic storage device and/or storage media is allowed to be connected in any manner (hardwired or wireless) to any County-owned computer/electronic device or to the County network for the purpose of transferring electronic information unless approved by the I.T Department and the department manager.

Only County-purchased hardware/software is allowed to be connected/installed to County-owned computer equipment and/or the County network. All software must be pre-approved by the I.T. Director prior to any installation on County- owned equipment.

An identified Guest wireless network is provided for employees to connect their personal devices to which will provide Internet access only. This is a best effort network provided for convenience of employees. The I.T. Director reserves the right to do traffic management on heavy bandwidth users on this network.

Connection of any wireless access point or hub/switch to the network is strictly prohibited unless approved by the I.T. Director and installed by the I.T. Department.

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 I.T. Department and/or the Elected Official or 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 I.T. Department to release a password for purposes of vendor support.

Violations

16. Employees violating this policy are subject to discipline, up to and including termination of employment. All reports of policy violation shall be reported to Human Resources for investigation.