

## **Policy Statement**

**TITLE**

**Information Technology Acceptable Use Policy**

**CODE**

**703**

**REFERENCE**

NA

**PERSONNEL RESPONSIBLE**

County Employees, Elected Officials

**EFFECTIVE**

Implemented: June 18, 1996

Revised: July 12, 2022

**703.100- PURPOSE**

- To clarify Yellow Medicine County's policy regarding use of the Internet and electronic mail
- To shield Yellow Medicine County against potential liability
- To avoid security threats by promoting awareness and good practice
- To safeguard and maintain strict confidentiality of private and confidential data including Individuals Identifiable Health Information (IIHI) and conform to Health Insurance Portability and Accountability Act (HIPAA)
- To ensure the integrity of data
- To encourage effective and positive use of our network, computer and electronic communication resources

**703.200- SCOPE**

Networked computers, Internet, public and private telephone systems have become a standard for communication between governmental organizations, commercial businesses and private citizens. In the process of communication traffic may cross multiple and different networks prior to reaching client destination. The public has a high reliance on the data shared from Yellow Medicine County; therefore it is our responsibility to insure the integrity of the data.

The variety of computing and electronic communication access tools that the County provides its employees include, but is not limited to, personal computers, laptops, networked servers, internal and external networks including wireless networks, electronic mail, voice mail, telephones, cellular/smart phones, modems and facsimile systems. These tools are County owned and publicly funded. The computer systems and software, peripherals, and the information conveyed through them are the property of the County. This Acceptable Use Policy

---

restricts access to and use of these systems. In addition, this policy applies to equipment that is the property of another entity or individual but is in use by County employees in the course of their employment with Yellow Medicine County. (e.g. telecommuters using their own personal equipment, county employees working for the county at another facility).

### **703.300- GENERAL PRINCIPLES**

Use of the Internet by County employees is permitted and encouraged where such use is suitable for business purposes and supports the goals and objectives of Yellow Medicine County and its departments. The Internet is to be used in a manner that is consistent with Yellow Medicine County's standards of business conduct and as part of the normal execution of an employee's job responsibilities.

### **703.400- INDIVIDUALS WHO ARE SUBJECT TO THIS POLICY**

This policy applies to all users of the County's electronic communications systems. Such individuals may include, but are not limited to, Yellow Medicine County Board members, elected officials, department heads, supervisors, employees, agents for the County, independent contractors doing work for the County, volunteers, and members of the public. By using any of the County's computer systems, telephones, voicemail, e-mail and Internet access users agree to be bound by the terms and conditions of this policy. Each individual user is responsible for complying with this policy.

Every employee who uses any County computer system will receive a copy of this policy and must sign the Employee Agreement, which is found in Appendix A of this Policy. The original copy of the signed agreement will be kept on file in each employee's personnel file.

### **703.500- COUNTY'S RIGHT TO INSPECT AND MONITOR ITS COMPUTER SYSTEMS AND COMPUTER SYSTEMS DATA**

The County is the sole and exclusive owner of the computer systems it provides and all computer system data. Use of the County's computer systems is a privilege, not a right. Accordingly, without further notice, the County and its individual department heads or supervisors reserve the right to use any means available to access, inspect, review, and monitor its computer systems and computer systems data including, but not limited to, computer files, e-mail, voice mail and Internet access information. In exercising this right, the County, its individual department heads and supervisors reserve the right to override any passwords and access codes that are on any of its computer systems. The County and its individual department heads or supervisors, and their designees, may also use software that assists in monitoring its computer systems and data on those systems.

Employees and other users shall have no expectation of privacy related to such use. This includes, but is not limited to e-mail and Internet access data. By using any of the County's computer systems, employees and other users consent to and understand that the County may access, monitor, and inspect any data that are received, sent, processed, stored, or transferred by means of any County computer or telephone system.

Users should consider e-mail and all other computer systems data to be a shared filing system, which may be accessed and reviewed by the applicable department head or supervisor at any time and without further notice. The County reserves the right to track and recover any computer systems data despite any attempt by a user to delete such data. Users are advised that all data can be tracked and recovered. For example, the County can track which websites

---

a user has visited, the time of day when the visits occurred, and how long each visit lasted. This information can be recovered even when the user has attempted to delete the information.

The County may use any computer system data for any purpose directly or indirectly related to County business, including ensuring compliance with this Policy and other professional and job related duties. Such data may also be used in deciding whether to impose discipline, and in disciplinary proceedings and civil and criminal litigation.

## **703.600- SYSTEM INTEGRITY**

### **703.601- Password Security:**

All employees are required to take reasonable precautions to protect the security of their passwords. Employees may not share passwords or user names, or use another person's password or user name when using a County computer system or accessing computer system data, unless prior permission has been received from the individual department head or supervisor. Absent prior permission from a department head or supervisor, no employee may knowingly permit another individual to use the employee's password to log onto or use any County Computer system.

If an individual department head or designee directs an employee to provide his or her passwords or access codes, the employee must immediately provide the current passwords and access codes.

Password policies are implemented using the following criteria: Minimum of 12 (Twelve) characters, Contain both upper and lower case characters (e.g., a-z, A-Z), Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&\*()\_+|~-=\`{}[]:;';<>?,./), Password changed every 90 days. The same password may be used every 365 days.

### **703.602- Modification of Default Settings:**

Employees may not modify assigned user names. Users may not modify any default settings on any County computer system (including hardware and software) without prior consent from the IT Coordinator.

### **703.603- Installation of Software:**

Employees may not install any software i.e. patches, upgrades, downloads, etc. on a County computer system without prior consent from the IT Coordinator. The County reserves the right to remove unauthorized software at any time and without prior notice.

Under no circumstance should screen saver programs or games (other than the games installed with the Windows OS) be installed on County owned computers. Bi-directional software, such as the 'Weather Bug' should not be installed on computer systems unless use of the product directly affects the workers employment at Yellow Medicine County. (e.g. Road Construction Crew) In all cases, consent must be written, approved and on file.

Executable files should not be downloaded and installed on County owned computers. Exception: Adobe Reader and WinZip are allowed with approval from the IT Coordinator.

Appropriate personal pictures may be emailed to County email addresses and used as desktop backgrounds and computer screensavers.

---

---

### **703.604- Commercial Access Providers:**

Users shall not use any Internet access or service provider other than the access or service provider that is supplied and made available to the user by the County.

Exception: Telecommuters will use their personal Internet service provider at their home location.

### **703.605 Use of Non-County Owned Assets (BYOD)**

Access to any County Information Technology resource is only permissible using methods and tools approved by Information Technology. All other means of access are prohibited.

Unless permission has been granted by the Information Technology Director and documented using the Policy Exceptions Procedure, employees and contractors must never conduct County work on personal or non-county email accounts. Personal use of County email is prohibited. To do so would circumvent control over the disposition of Government Data and potentially subject the County to data breaches and non-compliance with the Data Practices Act.

Personal digital assistants, handheld computers, and smartphones must not be used to access or store any not public data unless they have been approved for such use by Information Technology and configured with the necessary controls, such as encryption and boot protection, mobile device management (MDM).

Connecting unapproved, non-county owned assets to a Yellow Medicine County managed infrastructure, county network (not including the guest network) or resource without authorization is strictly prohibited.

#### **a. Camera Phones and Other Personal Recording Devices**

To protect not public data or other valuable assets from theft or misuse the use of video recorders or other devices for recording purposes is prohibited. Exceptions include: Sheriff's Office body cameras, recordings made of meetings, conferences or training sessions may be allowed with the permission of management and the agreement of those in attendance, or other job-related functions; the photographing or recording of other employees may be made on a limited basis at business-related social functions or at Yellow Medicine County sponsored events, and must have the permission of IT and/or the Department Heads involved.

No County data is to be stored on personal devices, all data must be transferred to a county-owned device or application and deleted from personal devices.

#### **b. Cell Phone and Electronic Devices**

Limited use of personal cell phones while on premises may be permitted as long as it does not interfere with performance, pose a distraction or create an unsafe situation for others. This policy applies to both incoming and outgoing cellular calls and includes sending and/or receiving text messages. All Yellow Medicine County employees, contractors, and vendors should be considerate by ensuring their cell phones do not ring in a distracting manner or otherwise interfere with the ability of others to perform work productively or for any services received by or for the public.

---

---

## **I. Remote Access & Teleworking**

All remote access to county resources whether on county assets or approved non-county owned assets must be approved and coordinated by Information Technology. County-owned access must only access County-resources through the approved VPN capability.

1. All mobile devices must enroll in the County-approved Mobile Device Management solution (e.g. Intune) before accessing county emails/calendar and data on their County-owned Devices.
2. All Devices must deploy continuous (always “on”) approved anti-malware and antivirus software and/or services that are approved by Information Technology.
3. The device must be able to satisfy the security policy requirements for lockdown, administrative access, password strength, encryption and automatic shut off.
4. Remote workers using County-owned devices are responsible for bringing County-owned devices into their respective offices or the Yellow Medicine County facility on a regular basis to receive updates and patches.
5. A device’s prolonged absence from direct Yellow Medicine County network connection is prohibited. The absences will be monitored and logged by the Information Technology security team. Violations will be reported to the Director of Information Technology.

### **703.700- ELECTRONIC MAIL (“E-mail”)**

#### **703.701- Application of Government Data Practices Act:**

All e-mail messages and attachments that are sent, received, or accessed by means of any County computer system, including any e-mail system, are County property and are subject to federal and state laws, such as the Minnesota Government Data Practices Act, which govern the collection, creation, storage, maintenance, dissemination, and access to data created or maintained by the County. All employees must exercise care in addressing messages to ensure that they are sent to the proper addressee.

**703.702- Warning:** All e-mail users are reminded that e-mails sent through the County’s electronic communications systems are documents with government data just as though sent and signed on County letterhead. Deleted e-mail is not necessarily deleted and could be used as damaging evidence against the County and/or the e-mail user.

#### **703.703- Temporary Storage Medium:**

The County’s e-mail system is meant to be a temporary medium for the transmission of data. All government data that is required to be maintained pursuant to law shall be maintained separate from the County’s e-mail system. All employees must transfer all such data to a different medium.

#### **703.704- Use of E-Mail by Non-Employees:**

Certain parts of the County’s e-mail system are open to state agencies, political subdivisions, and the public to provide a means by which members of state agencies, political subdivisions, and the public may communicate with the County. Individuals who subscribe to the County’s e-mail system must agree to comply with this Policy. Messages sent between the County and individuals that are not County employees may be used by the County for any purpose related to County business.

---

---

**703.705- Internet Access:**

Access to and use of the Internet through any County computer system is subject to the terms and conditions of this Policy. Access to and use of the Internet through any County computer system is limited to work related activities.

**703.706- Confidentiality Notice:**

All employees and elected officials must incorporate a Confidentiality Notice into all email messages.

**703.800- Clean Desk Guidelines and Physical Safeguards****a. Physical Safeguards**

Employees are expected to take the following physical safeguard measures:

1. Employees must ensure that workstations are secured when unattended either by logging off of the county network or using a password-secured screensaver.
2. Computers located in an area where the public may be in proximity must have monitors positioned in a way such that any not public data on monitors is not visible to the public. Use of screen protectors is recommended for monitors visible to the public and required for computers accessing Not Public data by regulations, statutes, and law.
3. Computers or any mobile device such as a laptop or Personal Digital Assistant (PDA) that are located in an area where there is access to the public must be physically secured to discourage theft.

**b. Clean Desk Guidelines**

Yellow Medicine County adheres to the Clean Desk Guidelines. The Clean Desk Guidelines takes into account the data classifications, legal and contractual requirements, and corresponding risks associated with exposure of not public data.

The Clean Desk Guidelines is based on industry best practices and includes the following:

1. Not public data (e.g., on paper or on electronic storage media) shall be locked away (ideally in a safe or cabinet or other forms of security furniture) when not in use, especially when the office is vacated;
  2. Computers and terminals shall be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism that conceals information previously visible on the display when unattended;
  3. Incoming and outgoing general office or publicly accessible mail points, printers, photocopiers, and unattended fax machines shall not receive or transmit not public data.
  4. Printers, copiers and fax machines that are authorized for not public data should be cleaned of all potential stored not public data before disposal or replacement;
  5. Documents containing not public data shall be removed from printers, copiers, and fax machines immediately; and
-

- 
6. When transporting documents with not public data within facilities and through inter-office mail, information shall not be visible.

### **703.900- UNACCEPTABLE USE OF THE COUNTY'S COMPUTER SYSTEMS, NETWORK OR COMMUNICATION SYSTEMS**

**Unacceptable use is defined as, but not limited to, the following:**

#### **1. Threatening or Fraudulent Messages**

No person may use any County computer system, network or communication system to intentionally or unintentionally threaten or offend another person or to send a fraudulent message.

#### **2. Harassment and Discrimination**

No person may use any County computer system, network or communication system to harass or discriminate against another person on the basis of race, color, creed, religion, national origin, sex, and marital status, status with regard to public assistance, disability, sexual orientation, or age. County computer systems, network, or communication systems may not be used to transmit, display, or distribute information on hate groups. All County policies on harassment and discrimination apply to conduct performed using any County computer system, network or communication system.

#### **3. Pornographic, Obscene, Vulgar, Lewd, and Sexually Explicit Material**

No person may use any County computer system to seek out access, upload, download, store, transmit, display, or distribute pornographic, obscene, vulgar, lewd, or sexually explicit language or material.

The sole exception to this rule is when such materials are directly related to the job duties of an employee as related to a specific case (e.g. law enforcement, child support and nursing services) and the employee has received **written permission** from the employee's supervisor to access or send such materials.

Employees must not send obscene, vulgar, lewd, and sexually explicit material through the County's e-mail system. Employees receiving such mail must direct the sender, if known, that it is against County policies to receive this type of mail and to remove the recipient from its address database.

#### **4. Harm to Reputation**

No person may use any County computer system to defame another or in a manner that harms the reputation of the County.

#### **5. Disruption**

No person may use any County computer system in a manner that damages, disrupts, or interferes with any County operation, service, equipment, or the job

---

---

performance of an employee. Such disruption or interference includes, but is not limited to, distribution of unsolicited or personal advertising and excessive downloading or transmission of programs or data.

## **6. Vandalism**

No person may use any County computer system to directly or indirectly vandalize, damage, or disable the personal, real, or intellectual property of another person or organization, or to make unauthorized modifications to the property of another (including information owned by the County). By way of example, this rule prohibits “hacking” into a County computer system or a private party’s system, as well as the propagation of computer worms and viruses.

## **7. Unauthorized Interception or Access**

No user may override another person’s passwords or codes or take any other action to intercept or access another person’s materials, or electronic information, or files (including e-mail) without the prior permission of that person. The exception to this rule is that a department head or supervisor, IT Department, or a person acting at the County management’s request to override passwords and may access, inspect, and monitor any computer systems data including, but not limited to, e-mail and information on Internet access.

## **8. Copyright Infringement**

No person may use any County computer system to violate any copyright law or otherwise use the intellectual property of another person or entity without proper authorization. The unauthorized duplication of computer software, downloading or exchanging of pirated or otherwise unlawful software constitutes copyright infringement and is strictly prohibited by this Policy. Only software licensed by the County is to be installed on County owned computer systems.

## **9. Commercial Use and Private Causes**

No person may use any County computer system for private commercial use, for personal financial gain, to promote any private cause (including but not limited to political or religious causes), or to enter into any contractual relationship without obtaining prior written authorization from the Yellow Medicine County Board of Commissioners. Similarly, no person may use any County computer in a manner that could reasonably result in any expense, financial loss, or obligation for the County. The County hereby disclaims any liability for any unauthorized financial obligation incurred by unacceptable use of its computer systems in violation of this rule. The exception to this rule is use of the electronic communication systems for benefits or fundraisers that directly benefit the health and well being of the Yellow Medicine County community (e.g. Relay for Life, wellness benefits for life threatening illnesses and catastrophic losses). All exceptions must be approved by the County Administrator.

## **10. Gambling**

No person may use any County computer system to gamble or engage in a game of chance for money or other valuable consideration.

---

---

## **11. Disguising Identity**

No person may disguise or attempt to disguise their identity while using any County computer system. For example, individuals may not disguise their identity while using a County computer system to send or receive information via e-mail or the Internet.

## **12. Violating the Law**

No person may use any County computer system in a manner that violates any local, state, or federal law or engage in any type of illegal activities.

No person may review or access any materials related to obtaining or using any controlled substances, **without the express written permission of their Department Head on file in the official personnel file of the employee.** For the Department Heads, permission must be received by the County Administrator.

## **13. Conduct Unbecoming**

No person may use any County computer system to engage in conduct unbecoming a County employee.

## **14. Chain Letter and Pyramid-Type Letters**

No person may use any County computer system to transmit or forward chain letters or pyramid-type letters. Any person receiving a chain letter or pyramid-type letter shall immediately direct the sender of the chain letter or pyramid-type letter to remove the recipient from its address database.

## **15. Private E-Mail Accounts and Instant Messaging Prohibited**

Employee must not access personal e-mail accounts through the County's computer systems. Accessing these systems bypass the County's antivirus and security applications.

The sole exception to this rule is when such materials are directly related to the job duties of an employee as related to a specific case (e.g. law enforcement, child support and nursing services) and the employee has received **permission** from the IT Department to access or send such materials.

## **16. Any other item(s) deemed unacceptable by Yellow Medicine County**

### **703.1000- Enforcement and Reporting Violations**

Compliance with this policy and all other policies at Yellow Medicine County is mandatory unless otherwise authorized via explicit written permission and documented according to the Policy Exceptions procedure. It is everyone's responsibility to read and understand all policies relevant to their job function and overall employment. The guidelines to this and all policies include some specific examples of prohibited use and requirements concerning the type of use and handling of information Those who violate any policy and/or its

---

accompanying guidelines may be subject to corrective action, which may include revocation of privileges, legal action, and/or severance of their relationship with Yellow Medicine County. In addition, those who violate this policy and accompanying guidelines may be subject to discipline up to and including discharge.

Yellow Medicine County reserves the right to hold individuals personally liable for any violations of policy when his or her conduct directly or through another person/entity results in a breach of confidentiality or security of not public data. Individual liability may include civil or criminal penalties.

Yellow Medicine County Information Technology employees are required to immediately report suspected violations of this policy to their supervisor, Department Head, or the IT Department.

A concern or complaint should be factual rather than speculative or conclusory and should contain as much specific information as possible to allow for proper assessment. The concern or complaint should be candid and set forth all of the information known and must contain sufficient corroborating information to support the commencement of an investigation. Anyone submitting intentionally false complaints will be subject to disciplinary action. The following information should be included to the extent reasonably possible:

- a. The alleged event, matter or issue that is the subject of the concern or complaint.
- b. The name of each person involved, if known.
- c. If the concern or complaint involves a specific event or events, the approximate date and location of each event.
- d. Any additional information, documentation or other evidence to support the concern or complaint.

The IT Department will maintain a log of all concerns and complaints, tracking their receipt, review, investigation, and resolution, and will prepare a periodic summary report thereof for the Human Resource Manager's Office. Copies of concerns and complaints and such log will be maintained.

Any suspected data breach must be reported immediately to the Information Technology Department and County Attorney's Office. Any suspected or confirmed violation of the Data Practices Policy must be immediately reported to the County Attorney's Office.

### **703.1100- PERSONAL USE OF COUNTY COMPUTER SYSTEMS BY EMPLOYEES**

#### **703.1101- Limited Personal Use Permitted:**

The County's computer systems are provided to support County business and, accordingly, are intended to be used primarily for business related purposes. Unless prohibited by the applicable department head, employees may engage in **incidental and occasional personal use** of the County's computer systems. Individual department heads may determine when an employee's personal use becomes excessive or otherwise violates this Policy. All personal use must be limited such that it:

- is done on the employee's personal time, and not on County time;
-

- 
- does not interfere with County business or the use of its computer systems;
  - does not interfere with the employee's job performance or activities;
  - is not for personal financial gain or other promotional activities;
  - is not for political or religious purposes that could suggest endorsement by the County
  - does not damage any of the County's computer systems;
  - does not result in the consumption of County resources
  - does not result in any expense, financial loss, or obligation for the County;
  - does not violate any rule set forth in this policy;
  - does not violate any federal, state, or local law;
  - does not violate any other policy of the County.

**Note: Minimal personal use of the County computer systems, network or communication systems, including Internet and e-mail, is a privilege for the employee only. No other family members or children of the employee are to use the County computer systems, network applications, e-mail or Internet for personal use.**

**703.1102- No Expectation of Privacy:**

Employees who use any County computer system for personal use have no expectation of privacy in any information that is stored, processed, or transferred by any of the County's computer systems, including but not limited to e-mail and information accessed on the Internet. Like any other data stored on the County's computer systems, data created from an employee's personal use is subject to periodic inspection and monitoring. **By engaging in personal use of any County computer system, employees and other users consent to such inspection and monitoring.**

**703.1200- CONSEQUENCES FOR VIOLATION OF THIS POLICY**

County management will review alleged violations of this Policy on a case-by-case basis. Any employee's failure to comply with any part of this Policy may result in disciplinary action up to and including termination of employment with the County, subject to the County Personnel Policy and any applicable collective bargaining agreement. In addition to any penalty or discipline imposed, any user's failure to comply with this Policy may result in loss of the privilege to continue using the County's computer systems and, if the violation is criminal in nature, referral to law enforcement.

**703.1300- QUESTIONS REGARDING THIS POLICY**

Employees who have questions about this Policy are required to present their questions to their department head or supervisor. If the supervisor is uncertain about the answer to the employee's questions, the department head or supervisor will submit the question in writing or email to the County Administrator and Information Technology Coordinator.

In consultation with the involved department head or supervisor, the County Administrator and Information Technology Coordinator will answer any questions about this Policy and the acceptable use of the County's computer systems. Until an answer is provided,

---

---

questionable use should be considered inappropriate and unacceptable. Implementation and interpretation of this Policy will be the responsibility of the County Administrator in consultation with the Information Technology Coordinator.

### **703.1400- NO EXPECTATION OF PRIVACY IN USE OF COUNTY PROPERTY AND EQUIPMENT**

The work areas, offices, desks, file cabinets, buildings, lockers, vehicles, equipment, telephone, voice mail, books, papers, computer systems, e-mail and all other property and systems of the County may be entered and searched and or reviewed by County personnel at any time without notice.

Employees, agents, independent contractors and all other individuals or entities using County property or equipment shall have no expectation of privacy in their use or possession of any property belonging to the County, including work areas, desks, e-mail accounts, computers, portable computer storage media, voice mail, papers books, etc., except as specifically provided by the Minnesota Government Data Practices Act. The County shall not be responsible for any alleged violations of employees' data privacy rights for data kept by the employee outside of secure, supervisory files.

Employees may be disciplined for any misuse of County property, including any unauthorized personal use. Such discipline may include, but is not limited to, reprimands, suspensions or discharge from employment, depending upon the nature and severity of the conduct. Employees may also be referred to law enforcement for criminal prosecution in the event that their use or misuse of County property constitutes or may constitute a crime.

Other individuals or entities misusing County property may be denied further access to such property, and may also be referred to law enforcement for criminal prosecution in the event that their use or misuse off County property constitutes or may constitute a crime.

### **703.1500 – PREVIOUS POLICIES REPLACED**

This policy replaces all computer and technology related acceptable use policies previously adopted by the County.

---

---

---

**APPENDIX A**

**YELLOW MEDICINE COUNTY  
INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY**

**EMPLOYEE AGREEMENT SIGNATURE**

**EMPLOYEE SIGNATURE:**

I have received a copy of Yellow Medicine County's "Information Technology Acceptable Use Policy" and agree to abide by the terms and conditions of this policy, and I understand the consequences for failing to do so. I further understand that my computer and e-mail use may be monitored at any time by my employer without further notice and consent to such monitoring and the release of the records of my computer, Internet and e-mail transactions to all appropriate authorities, including County officials and agents, civil and law enforcement authorities. I further agree to abide by all copyright laws and will not unlawfully copy software or other copyrighted materials owned or licensed by my employer or others and that if I do so, I will be subjected to disciplinary action, including possible termination of my employment, civil and criminal penalties. I consent to the release of any information related to possible copyright infringement to all appropriate authorities, including civil authorities, the attorney general's office and law enforcement authorities.

\_\_\_\_\_  
**Employee Signature**

\_\_\_\_\_  
**Date**

**Printed Name of Employee:** \_\_\_\_\_

---