1.7(1): Computer and Internet Use

This policy applies to all employees.

POLICIES AND PROCEDURES

Appropriate Use(s)

Employees must use good judgment and professionalism at all times when using the internet and other electronic communication tools. Electronic media is made available to provide an effective method to engage in work-related communication, and to perform job-related research tasks. However, access is a privilege that may be granted or revoked for individual employees by each Department Director or elected official.

Examples of appropriate use of electronic media may include the following:

- Accessing external resources to obtain work-related information.
- Disseminating County documents which are not privileged, protected, or confidential to other individuals or organizations.
- Participating in e-mail groups that may provide insight and assistance for work-related functions.
- Communicating with other County employees about work-related issues.
- Communicating with other professionals with similar jobs to share ideas and problem-solve.
- Obtaining information from vendors on products and services.

Prohibited Uses

Employees are prohibited from using electronic media for the following activities:

- Transmitting or soliciting any material or messages that would violate federal, state, and local law, regulation, or ordinance, or that would violate policies in section one of this employee manual.

- Distributing information that is privileged, protected, confidential or otherwise subject to nondisclosure under any law, regulation, or rule. If an employee is not sure whether information is confidential or privileged, the employee should consult with his or her Department Director or elected official, in addition to the County Attorney's Office, before distribution of such material.

1.7(1): Computer and Internet Use (continued)

- Distributing unauthorized broadcast messages or solicitations.
- Accessing or distributing pornographic materials.
- Distributing or downloading copyrighted materials in violation of the copyright, including software, photographs or any other media.
- Developing or distributing programs that are designed to infiltrate computer systems internally or externally.
- Accessing or downloading any resource that requires a fee without prior appropriate approval.
- Representing oneself as another user or employee.
- Attempting to access an unauthorized system.
- Attempting to access restricted content or bypass security restrictions by use of proxies or Virtual Private Networks (VPNs).
- Giving your password to someone without written supervisor approval that must be received by the ITi Department.
- Attempting to intentionally bypass security safeguards deployed on County systems and/or networks.
- Connecting County equipment to cellular networks (e.g. tethering or hotspots) in order to bypass County network protections.
- Connecting personally owned devices directly to the County network via Ethernet port (e.g., wall jack), Admin-Employee Wireless, or County issued equipment (e.g., USB, Ethernet or Bluetooth) without authorization from ITI Director. All personal devices must be authorized and comply with the Adams County Personal Computing Device Policy (BYOD): https://myadams/ITI/Pages/ITPolicies.aspx
- Using excessive bandwidth for non-business related tasks. Excessive bandwidth usage includes personal internet or network usage that interferes or disrupts with County operations. Excessive bandwidth usage could be a result of video and music streaming, large internet uploads or downloads, and cloud file storage services (e.g. DropBox and GoogleDrive). Users and/or managers will be notified by ITi if they are using excessive bandwidth. In an effort to protect County operations, and citizen access to County resources, ITi may temporarily block internet access from devices as necessary.

1.7(1): Computer and Internet Use (continued)

If an employee is in doubt whether or not an electronic media use is prohibited, the employee should consult with a supervisor, department director, elected official, or a representative from People and Culture Services. .

Security

Employees must protect data at all times against unauthorized access and ensure that information is handled in accordance of all applicable laws and regulations. Employees must immediately report any security incidents to the Information Technology Help Desk.

All employees with access to Adams County computer systems and/or data must complete the web-based security awareness training within ninety (90) days of employment.

To protect county data, users must handle data in compliance with the Adams County ITI policies and procedures, which are located at https://myadams/ITI/Pages/ITPolicies.aspx.

Employees who do not follow ITI policies and procedures in their use of County computer systems, or are otherwise negligent in regard to security procedures, will be subject to discipline, up to and including termination.

Cloud Based Storage and Transmission

Employees may only use cloud based storage to facilitate their ability to perform duties as an employee of Adams County. Employees must not use any form of cloud based storage as a primary or permanent storage mechanism; any final versions of work must be appropriately stored on Adams County networks.

Cloud based storage may not be used to store any sensitive or confidential information. Sensitive information for this purpose is any information that is not properly protected from unauthorized use and/or disclosure, and that could potentially damage the County, employees of the County, citizens, or any other interested parties. Confidential information includes social security numbers, medical information, information about child, and welfare cases; this type of information should never be stored on cloud based systems without explicit authorization from ITI.

Employees who use cloud based storage are responsible for ensuring that adequate protections are in place, such as password protection, to prevent cloud based information is protected.

For acceptable use of Adams County Office 365 for transmission and storage, see the Office 365 Policy at https://myadams/ITI/Pages/ITPolicies

1.7(1): Computer and Internet Use (continued)

Monitoring

The County reserves the right to access, monitor, and disclose the contents of employees' electronic messages, internet communications, and other information received or transmitted by electronic media. Circumstances in which accessing, monitoring, and disclosing will occur may include, but are not limited to:

- To investigate suspected misuse of electronic media;
- To respond to investigations that are related to pending or anticipated litigation;
- To ensure compliance with this policy, applicable laws, ordinances, or court orders;
- To ensure appropriate use for County business;
- To access information in the employee's computer system when the employee is unavailable;
- To investigate possible cyber security threats; and
- To respond to a request under the Colorado Open Records Act.

All requests for access to another employee's County email or electronic files must be made through ITI. The Director of People Services or designee must approve any request for access before such access is provided.

Personal Use

Incidental use of internet, personal e-mail, and/or personal networking sites may be permitted by a department director's or elected official's discretion. However, an employee's personal use of e-mail and/or internet must not interfere with his or her assigned duties or efficient use of time or must not conflict with other prohibitions in this policy.

Colorado Open Records Act/Public Records

The Colorado Open Records Act (CORA) requires that all public records, as defined by CORA, be available for inspection and replication by any member of the public. As such, a employee writings, records, and correspondence, whether in electronic or paper form, may be deemed to be public records subject to inspection under C.R.S. § 24-72-201 *et. seq.*.

Employees, who use cloud based document storage, must ensure that all public documents are appropriately stored on the existing Adams County technology network for purposes of inspection and disclosure to the public.

1.7(1): Computer and Internet Use (continued)

Violations

Violations of this policy may result in termination of access to the internet or other forms of electronic media. Violations may also result in disciplinary action, up to and including, termination of employment under the Discipline and Appeal Policy 1.8.