

Subject: INTERNET ACCESS AND USAGE

Date: May 17, 2017

Pages: 1 of 4

Replaces Policy Dated: April 10, 2007

PURPOSE: The purpose of this policy is to document employee responsibilities for the proper, secure, and lawful use of the Internet, via access provided by Pinal County with Pinal County equipment.

APPLICATION: This policy applies to all Pinal County employees.

This policy does not apply to public access to the Internet via the County's network from Public Libraries in Pinal County.

DEFINITIONS

Computer Virus: A software program capable of replicating itself and usually capable of causing great harm on the system that it invades.

Download: Means to receive data from another computer (often called a host computer or host system or host) into your computer. Download is also referred to as receive.

Intellectual Property: Rights and products of the mind or intellect, arising under any law, including but not limited to, Trade Secrets, Trademarks, Trade Dress, Copyrights, and Unfair Competition. This includes any body of work developed by an employee working on County business.

Internet: Thousands of interconnected networks originally developed by the military and referred to as the Internet, the Information Super Highway, the Net, the Web, or similar names.

Upload: To transmit a data file from your computer to another computer. Upload is also referred to as transmit.

POLICY

1. Internet access to global electronic information resources is provided by Pinal County to assist employees in work-related matters. This includes use of the Internet to provide information to County residents, businesses and other governmental agencies; to encourage teamwork, networking and interagency support; to search for information; and, for information exchange. Use of the internet for personal, non-work related matters is prohibited.
2. Employees are not to use their own personal Internet accounts or use Pinal County equipment to reach personal sites during work hours without the prior written authorization of their Appointing Authority. Pinal County Internet access is limited to business purposes during business hours.
3. Employees are responsible for protecting their Pinal County Internet access that has been entrusted to them.
4. The possibility of downloading a file with a computer virus exists, therefore, care must be taken not to contaminate or compromise any computers in the County network. Files downloaded from the Internet,

or any other outside service, must be scanned by a virus checking software prior to being used on a County computer. Elected Officials or Department Heads should contact Management Information Services for options available for virus checking of downloaded files and training.

5. Employees should take extreme care when uploading files to the Internet. Files uploaded to the Internet are not secure and can be intercepted by persons other than the intended recipient(s).
6. All data composed, sent, or received via County Internet access or on County computers or computer linked equipment is the property of Pinal County. All such electronically composed data is the intellectual property of Pinal County and is not the private property of any employee.
7. Data composed, transmitted, accessed, or received via the County provided Internet access are considered Public Records, unless it falls into an exemption recognized by statute and/or law.
8. All Internet data that is composed, transmitted, or received via the County's computer equipment is considered to be part of the official records of Pinal County and, as such, may be subject to disclosure to law enforcement or other third parties. Consequently, employees should always ensure that the business information contained in Internet e-mail messages and other transmissions is accurate, appropriate, ethical, and lawful.
9. Except as noted in bullet 10 below, the County reserves the right to review, audit, intercept, access and disclose all data composed, transmitted, accessed, or downloaded via County provided Internet access. The contents of Internet data properly obtained for legitimate business purposes may be disclosed without the notice or permission of the sender. Notwithstanding the County's right to retrieve and read any Internet messages, such messages shall be treated as confidential by other employees and accessed only by the intended recipient. No Internet messages may be monitored, reviewed, audited, intercepted, accessed, or disclosed without authorization of the County Manager or designee.
10. No electronic messages created, received or sent over the Internet by any employee or agent of the Pinal County Attorney may be monitored, reviewed, audited, intercepted accessed or disclosed without the prior written authorization of the Pinal County Attorney or his designee. This Policy complies, in all respects, with the provisions of the Rules of the Supreme Court, Rule 42, Professional Conduct, including, but not limited to the provisions of ER 1.6, Confidentiality of Information.
11. Employees have no right of privacy, nor any expectation of any right to privacy, when accessing the Internet by use of County equipment. The County reserves the express right to monitor, in any way, the activities of the employee while accessing the Internet. Violation of County policy regarding Internet use may result in disciplinary action up to and including dismissal.
12. Prohibited uses of Pinal County Internet access include, but are not limited to:
 - A. Composing, transmitting, accessing, or receiving data via the Internet that contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating or disruptive to any employee or other person.
 - B. Soliciting or recruiting membership for commercial ventures, religious or political causes, outside organizations, or other solicitations.
 - C. Composing, transmitting, accessing, or receiving data which contain sexual implications or comments that offensively addresses race, color, religion, gender, national origin, ancestry, marital status, sexual orientation, age, physical or mental disability, medical condition, or veteran status.
 - D. Composing, transmitting, accessing, or receiving graphic images that are not directly related to

County business.

- E. Composing, transmitting, accessing, or receiving serial or chain mail@ type messages or advertisements of any commercial nature.
 - F. Sending (uploading) or receiving (downloading) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.
 - G. Attempting to gain access to another employee's messages or files without his/her permission.
 - H. Any activity that violates established County or department policy.
13. Any employee who discovers a violation of this Policy shall notify their Appointing Authority who may request an investigation by the Human Resources Director.
14. Any employee who violates this policy or uses the Internet for improper purposes shall be subject to discipline, up to and including discharge.

AUTHORITY AND RESPONSIBILITY:

1. Employees are responsible for:
 - A. Understanding and adhering to the Internet Access and Usage policy.
 - B. Using common sense and good judgment in the use of the Internet as determined by this County Policy and the Director of Information Technology.
 - C. Advising Management of breaches of this policy.
 - D. Maintaining reasonable precautions to safeguard their Internet access from unauthorized entry or use.
2. Management is responsible for:
 - A. Understanding this policy, and related policies and documents
 - B. Advising their employees about this policy and appropriate use.
 - C. Management Information Services will monitor and record user access to the Internet and provide the Elected Official or Department Head with information that can be used to track access to all Internet sites on a regular basis.
 - D. Monitor and audit use of the Internet within the department. Much like the County telephone system, there is the potential for employee abuse of the system.
 - E. Notifying the Director of Information Technology when circumstances warrant monitoring of an employee's Internet access and activity.
 - F. Establishing retention schedules in accordance with applicable statutes, County and organizational policies.
3. The Human Resources Director is responsible for:
 - A. Confirming that reported circumstances warrant monitoring.
 - B. Obtaining authorization from the County Manager or designee before monitoring specific activity.
 - C. Contacting the Information Technology Director to effect the monitoring
 - D. Reporting violations of this policy to the employee's Appointing Authority for further investigation and disciplinary action as appropriate.
 - E. Facilitating the use of external resources including civil or criminal investigators, as appropriate.

PROCEDURES

1. Authorized employees shall have access to the Internet via County computer equipment. All County workstations with Internet access will be provided with an internal virus scanning mechanism.

2. If a violation of this policy occurs or is suspected, the appointing authority or designee should:
 - A. Document the circumstances.
 - B. Confirm with the Human Resources Director that monitoring Internet access and usage is appropriate.
 - C. Monitor the employee's Internet access and usage in a manner consistent with the circumstances of the policy violation.
 - D. Initiate disciplinary action, as appropriate under the circumstances.