MARILYN EDWARDS
County Judge

280 North College, Suite 500
Fayetteville, AR 72701

WASHINGTON COUNTY, ARKANSAS
County Courthouse

August 30, 2013

MEETING OF THE
WASHINGTON COUNTY QUORUM COURT
COUNTY SERVICES COMMITTEE

Tuesday, September 3, 2013
5:30 p.m.
Washington County Quorum Court Room

AGENDA

1. Call to Order.
2. Adoption of Agenda.
3. Report from the Washington County Planning Office.
4. General Overview of the County's Environmental Affairs Office – Sophia Stephenson, Director
5. Report on Southeast Phase II Water Project.
6. Lester C. Howick Animal Shelter Report.
7. An Ordinance Amending Washington County Code Sections 2-62 Through 2-62.6 Pertaining To Computer Usage, Electronic Mail And Internet Security Policy. This is being brought to the Committee by County Computer Director John Adams. (7.1)
8. Other Business.
9. Public Comment.
10. Adjournment.

/kb

ORDINANCE NO. 2013-_____

BE IT ORDAINED BY THE QUORUM COURT OF THE COUNTY OF WASHINGTON, STATE OF ARKANSAS, AN ORDINANCE TO BE ENTITLED:

AN ORDINANCE AMENDING WASHINGTON COUNTY CODE SECTIONS 2-62 THROUGH 2-62.6 PERTAINING TO COMPUTER USAGE, ELECTRONIC MAIL AND INTERNET SECURITY POLICY.

WHEREAS, in 2002 the Quorum Court enacted a policy concerning computer usage, electronic mail, and internet security policy; and,

WHEREAS, due to the passage of time and changes in technology such policy needs to be updated and expanded.

NOW, THEREFORE, BE IT ORDAINED BY THE QUORUM COURT OF WASHINGTON COUNTY, ARKANSAS:

ARTICLE 1. Washington County Code Sections 2-62 through 2-62.6 is hereby amended to read as follows:

~~**Sec. 2-62. - Computer Usage, Electronic Mail, and Internet Security Policy—Purpose.**~~

~~The purpose of the Computer Usage, Electronic Mail, and Internet Security Policy document is to:~~

~~(1) Present an overall description of Washington County's Computer Usage, Electronic Mail, and Internet Security Policy;~~
~~(2) Describe the handling of electronic documents; and~~
~~(3) Identify each user's responsibilities with regard to the use of County-owned or supported computers, the handling of e-mail, and the Internet.~~

~~*(Ord. No. 2002-6, Arts. 1—3, 2-14-02)*~~

~~***Editor's note**— Ord. No. 2002-6, Arts. 1—3, adopted Feb. 14, 2002, did not specifically amend the Code; hence, inclusion as §§ 2-62—2-62.6 was at the discretion of the editor.*~~

~~**Sec. 2-62.1. - Responsibilities of Washington County and its computer users.**~~

~~(a) *Opportunities and risks.* The wide array of resources, services and interconnectivity available via the Internet introduce new opportunities and risks. In response to these risks,~~

~~this document details Washington County's official policy regarding computer usage, e-mail, and Internet security.~~

~~(b) *Applicability.* This policy applies to everyone (employees, contractors, temporaries, state employees, federal employees, elected officials, etc.) who uses Washington County computing or networking resources, as well as those who represent themselves as being connected in one way or another with Washington County. Washington County computing or network resources are defined as computers and related equipment purchased with County funds, attached to the County's network, or supported by County Computer Systems staff. All users are expected to be familiar with and comply with this policy. Questions about the policy should be directed to the Computer Systems Administrator.~~

~~(c) *County property.* As a productivity enhancement tool, Washington County encourages the business use of electronic communications (notably the Internet and e-mail). Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of Washington County.~~

~~(d) *Computing equipment and software purchases.* In order to more efficiently maintain and support Washington County's computer systems and network and to maximize value for money spent, minimum standards for computing equipment and software have been developed. Each computing equipment or software purchase should be made using a Washington County purchase order to assure that these minimum standards are met.~~

~~(e) *Use without authorization prohibited.* No one shall connect with or otherwise use any County computer, modem, network, or other computing resource without proper authorization; or assist in, encourage, or conceal any unauthorized use, or attempted unauthorized use, of any County computer, modem, network or computing resource; or misrepresent his or her identity or relationship to the County to obtain access to computing resources.~~

~~(f) *Authorized usage.* Washington County electronic communications systems must generally be used only for business activities. Incidental personal use is permissible so long as it does not consume more than a trivial amount of resources and does not preempt any business activity. Users are forbidden from using the County's electronic communication systems for chain letters, charitable endeavors, private business activities, political activities or amusement/entertainment purposes. Electronic mail attachments are to be used for business purposes only because they consume large amounts of computer resources and can easily be infected with viruses. For the same reasons, downloading files from the Internet is prohibited without the express consent of the Computer Systems Department. Use of County computing resources for game playing of any kind is prohibited. Users are reminded that the use of County resources, including computing resources and electronic communications, should never create either the appearance or the reality of inappropriate use.~~

(g) *Default privileges.* The privileges of using computing and electronic communications systems are assigned such that only those capabilities necessary to perform a job are granted. For example, end-users are not allowed nor able to reprogram electronic mail system software. With the exception of emergencies and regular system maintenance notices, broadcast facilities must be used only after the permission of an elected official or department head has been obtained. End-users may not install hardware or software or alter their user interface without the approval of the Computer Systems Department.

(h) *User accountability.* Regardless of the circumstances, individual passwords must never be shared or revealed to anyone besides the authorized user. To do so exposes the authorized user to responsibility for actions the other party takes with the password. If users need to share computer resident data, they should utilize message forwarding facilities, public directories on local area network servers and other authorized information sharing mechanisms. To prevent unauthorized parties from obtaining access to the County's network, users must shutdown their computer when leaving their workstation for extended periods and at the end of the day and choose passwords which are difficult to guess (for example, not a dictionary word, not a personal detail and not a reflection of work activities).

(i) *Disclosing confidential information.* Users must not publicly disclose confidential information via the Internet or e-mail.

(j) *Copyrights.* Washington County strongly supports strict adherence to software vendor's license agreements. When at work or when County computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Likewise, off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with County work and are, therefore, prohibited. Similarly, the reproduction, forwarding, or, in any other way, republishing or redistributing words, graphics or other materials must be done only with the permission of the author/owner. Users should assume that all materials on the Internet are copyrighted unless specific notice states otherwise.

(Ord. No. 2002-6, Arts. 1—3, 2-14-02)

Sec. 2-62.2. - Privacy expectations for electronic communications.

(a) *Respecting privacy rights.* Except as otherwise specifically provided, users may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. Washington County is committed to protecting the rights of its computer users, including their reasonable expectation of privacy. However, Washington County also is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

(b) *No default protection.* Computer users are reminded that Washington County's electronic communications systems are not encrypted by default. If sensitive information

must be sent by electronic communications systems, encryption or similar technologies to protect the data must be employed.

(c) *No guaranteed message privacy.* Washington County cannot guarantee that electronic communications will be private. Users should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed and stored by others. Furthermore, electronic communications can and, occasionally, will be accessed by others.

(d) *The Arkansas Freedom of Information Act.* The electronic files, including e-mail files, stored on Washington County computing systems are potentially subject to public inspection and copying under the state Freedom of Information Act (FOIA). The FOIA defines public records to include "data compilations in any form, required by law to be kept or otherwise kept, . . . which constitute a record of performance or lack of performance of official functions which are or should be carried out by a public official or employee [or] a governmental agency. . . ." All records maintained in public offices or by public employees within the scope of their employment are presumed to be public records. Various exceptions apply. Any (FOIA) requests for electronic files submitted to the Computer Systems Administrator will be forwarded immediately to the user who authored or received the file.

(e) *Regular message monitoring.* It is not the policy of Washington County to regularly monitor the content of electronic communications. However, the usage of electronic communications systems will be monitored for volume of traffic to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that Washington County may, from time to time, examine the content of electronic communications strictly for the purposes mentioned above.

(f) *Incidental disclosure.* It may be necessary for technical support personnel to review the content of an individual user's communications during the course of problem resolution. Technical support personnel may not review the content of an individual user's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels.

(g) *Internet activity logging.* For statistical purposes, Washington County routinely logs Web sites visited, time spent on the Internet, traffic levels and related information. This information will be used to determine expansion needs before critical traffic levels are reached in order to maintain optimal system conditions.

(Ord. No. 2002-6, Arts. 1—3, 2-14-02)

Sec. 2-62.3. - Computer security.

(a) *Security responsibilities.* No one shall knowingly endanger or compromise the security of any County computer, network facility, or other computing resource or willfully interfere with others' authorized computer usage; or attempt to circumvent data protection schemes, uncover security loopholes, or decrypt secure data; or modify or reconfigure, or attempt to modify or reconfigure, any software or hardware of any County computer or network facility

~~in any way, unless specific authorization has been obtained from the Computer Systems Department; or use County computer resources and communication facilities to attempt unauthorized access to or use of any computer or network facility, no matter where located, or to interfere with others' legitimate use of any such computing resource.~~

~~(b) *Problem notification process.* E-mail is the preferred method of communication with the Computer Systems Department, when possible. If it is not possible to use e-mail, telephone the Help Desk and leave a message containing a detailed description of your situation.~~

~~If sensitive information is lost or disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the Computer Systems Administrator must be notified immediately. If any unauthorized use of the County's computer or network systems has taken place, or is suspected of taking place, the Computer Systems Administrator must likewise be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the Computer Systems Administrator must be notified immediately. Because it may indicate a computer virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages and the like must also be reported. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.~~

~~*(Ord. No. 2002-6, Arts. 1—3, 2-14-02)*~~

~~Sec. 2-62.4. - E-mail policy.~~

~~(a) *Contents of messages.* Users must not use profanity, obscenities or derogatory remarks in electronic mail messages. Such remarks, even when made in jest, may create legal problems for the author and/or the County. Special caution is warranted because back-up and archival copies of electronic mail may actually be more permanent and more readily accessed than traditional paper communications.~~

~~(b) *Message forwarding.* Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. Sensitive information must not be forwarded without the approval of an elected official or a department head.~~

~~(c) *User back-up.* If an electronic mail message contains information relevant to the completion of a business transaction, contains potentially important reference information or has value as evidence of an elected official's or department head's decision, it should be retained for future reference. Most electronic mail messages will not fall into these categories and, accordingly, can be erased after receipt. Users must regularly move important information from electronic mail message files to word processing documents, databases, and other files. Electronic mail systems are not intended for archival storage of important information. Important stored electronic mail messages can be periodically expunged by system administrators, mistakenly erased by users and otherwise lost when system problems occur.~~

(d) *Purging electronic messages.* Messages no longer needed for business purposes must periodically be purged by users from their personal electronic message storage areas. After a certain period (generally six (6) months), electronic messages stored on multi-user systems will be automatically deleted by systems administration staff. The users will be notified before the messages are purged.

(e) *Harassing or offensive materials.* Washington County's computer and communications systems are not intended to be used for, and must not be used for, the exercise of the users' right to private or personal free speech. Harassment of any kind, especially harassment based on color, religion, age, sex (whether or not of a sexual nature), national origin, disability, veteran status, or any other protected status, including electronic mail and Internet mail, is strictly prohibited and is cause for disciplinary action up to and including termination. Users are encouraged to politely respond directly to the originator of offensive electronic mail messages. If the originator does not promptly stop sending offensive messages, users must report the communications to their supervisor and the appropriate elected official or department head. Washington County retains the right to remove from its information systems any material it views as offensive or potentially illegal.

(f) *Paper confirmation for contracts.* All contracts formed through electronic offer and acceptance messages (EDI, electronic mail, etc.) must be formalized and confirmed via paper documents and follow the same procedures for approval as all other contracts. Separately, because it may facilitate fraud, users must not employ scanned versions of hand-rendered signatures to give the impression that an electronic mail message or other electronic communications were signed by the sender.

(Ord. No. 2002-6, Arts. 1—3, 2-14-02)

Sec. 2-62.5. - Internet policy.

(a) *Access to the Internet.* Access to the Internet will be provided to each Washington County computer user who has access to a PC and the County's network if it is deemed appropriate by the elected official or department head who supervises the user. The ability to surf the Web and engage in other Internet activities is not a fringe benefit. Internet access is provided for business needs only. All connections to the Internet must pass through Washington County's firewall. For security reasons, no stand-alone Internet connection is allowed into or out of the County's network.

(b) *Internet content filtering.* Washington County reserves the right to block access to specific Web pages for the following reasons:

(1) To define and enforce access privileges;

(2) To protect against potential legal action;

(3) To preserve bandwidth and server space; and

(4) To manage Internet resources.

(c) *Information integrity.* All information taken off the Internet should be considered suspect until confirmed by separate information from another source considered to be reliable. There

~~is no general quality control process on the Internet and a considerable amount of its information is outdated, inaccurate and, in some instances, even deliberately misleading.~~

~~(d) *Virus checking.* All files residing on Washington County's computing or network resources are subject to anti-virus screening. Infected files will be deleted as soon as they are discovered. To help protect from viruses, downloading of files from the Internet or sharing files by floppy disk without the consent of the Computer Systems Department is prohibited.~~

~~(e) *Push technology.* Automatic updating of software or information on Washington County's computers via background "push" Internet technology is prohibited unless the involved vendor's system has first been tested and approved by the Computer Systems Department. While powerful and useful, this new technology could be used to spread viruses and cause other operational problems such as system unavailability.~~

~~(f) *User anonymity.* Misrepresenting, obscuring, suppressing or replacing a user's identity on the Internet or any Washington County electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation and related information included with messages or postings must reflect the actual originator of the messages or postings. If users have a need to employ remailers or other anonymous facilities, they must do so on their own time, with their own information systems and with their own Internet access accounts.~~

~~(g) *Web page changes.* Users may not establish new Internet Web pages dealing with Washington County unless they have first obtained approval of their department head or elected official and the approval of the Computer Systems Department. The Computer Systems Department has the overall responsibility to see that all posted material has a consistent and polished appearance, is pertinent and proper information for the County's website, and is protected by adequate security measures.~~

~~(h) *Message interception.* Wiretapping and other types of message interception are frequently encountered on the Internet. Accordingly, Washington County's confidential or private information must not be sent over the Internet unless it has first been encrypted by approved methods.~~

~~(i) *Appropriate behavior.* To avoid libel, defamation of character and other legal problems, whenever any affiliation with Washington County is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited. Likewise, users must not make threats against another user or organization over the Internet. All Internet messages intended to harass, annoy or alarm another person are similarly prohibited.~~

~~(j) *Internet Service Providers (ISP).* Users must not employ non-County Internet Service Provider (ISP) accounts and dial-up lines to access the Internet or electronic mail with Washington County computers. Instead, all Internet and electronic mail activity must pass through Washington County's firewalls so that access controls and related security mechanisms can be applied.~~

~~(k) *Establishing network connections.* Unless the prior approval of the Computer Systems Administrator has been obtained, users may not establish Internet or other external network connections that could allow non-Washington County users to gain access to Washington County systems and information.~~

~~These connections include the establishment of multi-computer file systems (like Sun's NFS), Internet Web pages, FTP servers and the like.~~

~~*(Ord. No. 2002-6, Arts. 1—3, 2-14-02)*~~

~~Sec. 2-62.6. - Computer Usage, Electronic Mail, and Internet Security Policy revisions.~~

~~Washington County reserves the right to revise this document as it sees fit to accommodate new technologies and the needs of its citizens and computer users.~~

~~*(Ord. No. 2002-6, Arts. 1—3, 2-14-02)*~~

Section 2-62. Overview

(a) Though there are a number of reasons to provide a user network access, by far the most common is granting access to employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the county network. This policy explains how information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus, the user is asked additionally to use common sense when using Washington County resources. Questions on what constitutes acceptable use should be directed to the user's supervisor. Questions from supervisors shall be directed to the Information Technology (IT) Department.

Section 2-62.1- Purpose

(a) Since inappropriate use of the county network exposes Washington County to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of information technology resources for the protection of all parties involved.

Section 2-62.2- Scope

(a) This policy applies to everyone (employees, contractors, temporaries, state employees, interns, federal employees, vendors, auditors, elected officials, etc.) who uses Washington County computing or networking resources, as well as those who represent themselves as being connected, in one way or another, with Washington County. Washington County computing or network resources are defined as computers and related equipment purchased with County funds, attached to the County's network, or supported by County Information Technology Systems staff. All users are expected to be familiar with and comply

with this policy. Questions about the policy should be directed to the Washington County IT Director.

(b) When the term "employee" or "user" is used it shall mean all persons covered by this Ordinance as stated above.

Section 2-62.3- Policy

(a) E-mail Use

Personal usage of Washington County email systems is permitted as long as:

1) Such usage does not negatively impact the computer network; and,
2) Such usage does not negatively impact the user's job performance.

(b) The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.

(c) The user is prohibited from forging email header information or attempting to impersonate another person.

(d) Email is an insecure method of communication, and thus, information that is considered confidential or proprietary to Washington County may not be sent via mail, regardless of the recipient, without proper encryption.

(e) It is Washington County's policy not to open email attachments from unknown senders, or when such attachments are unexpected.

(f) Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

(g) Please note that detailed information about the use of email may be covered in Washington County's Email Policy.

Section 2-62.4- Confidentiality

(a) Confidential data must not be

1) Shared or disclosed in any manner to non-employees of Washington County,
2) Should not be posted on the Internet or any publicly accessible systems, and
3) Should not be transferred in any insecure manner.

Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.

Section 2-62.5-Network Access

(a) The user should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access. No employee, consultant, or vendor, regardless of job function, will attempt to test any security of the county's system. Failure to follow this policy will result in loss of privilege.

Section 2-62.6- Unacceptable Use

(a) The following actions shall constitute unacceptable use of the network. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the network and/or systems to:

1) Engage in activity that is illegal under local, state, federal, or international law.

2) Engage in any activities that may cause embarrassment, loss of reputation, or other harm to Washington County.

3) Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.

4) Engage in activities that cause an invasion of privacy.

5) Engage in activities that cause disruption to the workplace environment or create a hostile workplace.

6) Make fraudulent offers for products or services.

7) Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of employee's job function.

8) Install or distribute unlicensed or "pirated" software.

9) Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

Section 2-62.7- Blogging and Social Networking

(a) Officially sanctioned social sites can be approved by Washington County elected officials this approval must be provided in writing to the Washington County IT

Department. No blogging or social networking is allowed from Washington County computers. Any access to approved sites must be accomplished on non-county equipment.

Blogging and social networking by Washington County's employees are subject to the terms of this policy, whether performed from Washington County's' network or from personal computer systems. In no blog or website, whether county or personal, will Washington County employees be identified, Washington County, or any Washington County business matters shall not discussed. Any material detrimental to Washington County shall not be published. The user must not identify himself or herself as an employee of Washington County in a blog or on a social networking site. The user assumes all risks associated with blogging and/or social networking.

Section 2-62.8- Instant Messaging IM (Jabber)

(a) Employees are prohibited from downloading and using personal, consumer-grade IM software (e.g., AOL Instant Messenger, Yahoo!, or MSN) to transmit messages via the public Internet.

(b) All IM communications and information transmitted, received, or archived in the company's IM system belong to Washington County.

(c) Employees have no reasonable expectation of privacy when using the county's IM system. The county reserves the right to monitor, access, and disclose all employee IM communications.

(d) The IM system is intended for business use only. Employees are prohibited from wasting computer resources, colleague's time, or their own time sending personal instant messages or engaging in unnecessary chat related to business.

(e) Treat IM messages as business records that may be retained and used as evidence in litigation, Audits, FOIA, and investigations.

(f) Always use professional and appropriate language in all instant messages. Employees are prohibited from sending abusive, harassing, threatening, menacing, discriminatory, pornographic, disrespectful, or otherwise offensive instant messages.

(g) Employees are prohibited from sending jokes, rumors, gossip, or unsubstantiated opinions via IM. These communications, which often contain objectionable material, are easily misconstrued when communicated electronically.

(h) Employees may not use IM to transmit confidential, proprietary, personal, or potentially embarrassing information about the county, employees, clients, business associates, or other third parties.

(i) Employees may not share confidential, proprietary, or potentially embarrassing business-related or personal IMs with the media, competitors, prospective employers, or other third parties.

Section 2-62.9- Overuse

(a) Actions detrimental to the computer network or other resources, or that negatively affect job performance are not permitted and will be restricted.

Section 2-62.10- Web Browsing

(a) The Internet is a network of interconnected computers of which Washington County has very little control. The employee should recognize this when using the Internet, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet at his or her own risk. Washington County is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

(b) Washington County recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of Washington County computer systems to access the Internet is permitted during lunch, breaks, and before/after business hours, as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on Washington County or on the users' job performance.

Section 2-62.11- Copyright Infringement

(a) Washington County's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner:

1) Copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's;

2) Posting or plagiarizing copyrighted material; and,

3) Downloading copyrighted files which employee has not already legally procured.

(b) This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above.

Section 2-62.12- Peer-to-Peer File Sharing

(a) Peer-to-Peer (P2P) networking is not allowed on the network under any circumstance.

Section 2-62.13- Streaming Media

(a) Streaming media can consume a great deal of network resources and thus must be used carefully. Streaming media is allowed for job-related functions only. Business cases for access must be submitted to the Washington County IT department for evaluation.

Section 2-62.14- Monitoring and Privacy

(a) Users should expect no privacy when using the county network or Washington County resources. Such use may include, but is not limited to: transmission and storage of files, data, and messages. Washington County reserves the right to monitor any and all use of the computer network. To ensure compliance with Washington County policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

Section 2-62.15- Bandwidth Usage

(a) Excessive use of Washington County bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low Washington County usage.

Section 2-62.16- Personal Usage

(a) Personal usage of Washington County computer systems is permitted during lunch, breaks, and before/after business hours, as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on Washington County or on the users job performance and the supervisor authorized such use.

Section 2-62.17- Remote Desktop Access

(a) Use of non-Washington County-supplied remote desktop software and/or services (such as Citrix, VNC, GoToMyPC, etc.) is prohibited, without written permission by the Washington County IT Director or his appointee. All requests for such access will be submitted in the Track-it ticketing system to Washington County IT.

Section 2-62.18- Circumvention of Security

(a) Using Washington County-owned or Washington County-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited. No person is authorized to test any security mechanism on any Washington County System. Any Actions to circumvent security or test security of Washington County system will be reported to the appropriate law enforcement agency for legal actions.

Section 2-62.19 Use for Illegal Activities

(a) No Washington County-owned or Washington County-provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

(1) Unauthorized Port Scanning

(2) Unauthorized Network Hacking

(3) Unauthorized Packet Sniffing

(4) Unauthorized Packet Spoofing

(5) Unauthorized Denial of Service

(6) Unauthorized Wireless Hacking

(7) Acts of Terrorism

(8) Identity Theft

(9) Spying

(10) Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system

(11) Downloading, storing, or distributing violent, perverse, pornographic, obscene, lewd, or offensive material.

(12) Downloading, storing, or distributing copyrighted material

(b) Washington County will take all necessary steps to report and prosecute any violations of this policy.

Section 2-62.20- Non-Washington County-Owned Equipment

(a) Permission to access Washington County's system with personal computer system must be approved by the Washington County IT Director or his appointee.

Section 2-62.21-Personal Storage Media

(a) Washington County does restrict the use of personal storage media, which includes, but is not limited to: USB or flash drives, external hard drives, personal music/media players, and CD/DVD writers, provided that guidelines for data confidentiality are followed. The user must take reasonable precautions to ensure viruses, Trojans, worms, malware, spyware, and other undesirable security risks are not introduced onto the Washington County network.

Section 2-62.22- Software Installation

(a) Installation of non-Washington County-supplied programs is prohibited. Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance. All requests for software installation will follow Washington County purchasing policy, which necessitates all requests to be submitted to IT for approval. No individual is allowed to download any software or install software application, regardless of the business need, without request submission to IT. Washington County will take all necessary steps to report and prosecute any violations of this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to, and including, termination of employment.

Section 2-62.23- Reporting of Security Incident

(a) If a security incident or breach of any security policies are discovered or suspected, the user must immediately notify his or her supervisor and/or follow any applicable guidelines as detailed in the Incident Response Policy. Examples of incidents that require notification include:

(1) Suspected compromise of login credentials (username, password, etc.).

(2) Suspected virus/malware/Trojan infection.

(3) Loss or theft of any device that contains Washington County information.

(4) Loss or theft of ID badge or keycard.

(5) Any attempt by any person to obtain a user's password over the telephone or by email.

(6) Any other suspicious event that may impact Washington County's information security.

(b) Users must treat a suspected security incident as confidential information, and report the incident only to his or her supervisor. Users must not withhold information relating to a security incident or interfere with an investigation.

Section 2-62.24- Applicability of Other Policies

(a) This document is part of Washington County's cohesive set of security policies and/or ordinances. Other policies may apply to the topics covered in this document, and as such, the applicable policies should be reviewed as needed.

Section 2-62.25- Enforcement

(a) Violations of this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to, and including, termination of employment. Washington County IT can and may restrict access to county systems as deemed necessary for violation of this policy. Where illegal activities or theft of Washington County property (physical or intellectual) is suspected, Washington County may report such activities to the applicable authorities.

Section 2-62.26- Definitions

(a) Blogging. The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").

(b) Instant Messaging. A text-based computer application that allows two or more Internet-connected users to "chat" in real time.

(c) Peer-to-Peer (P2P) File Sharing. A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

(d) Remote Desktop Access. Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

(e) Streaming Media Information. Typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

ARTICLE 2. This Ordinance shall be distributed by the Human Resources Office to all current and future elected officials and employees.

ARTICLE 3. A willful violation of this policy, after having received one warning, shall be punishable by a fine not to exceed Two Hundred Fifty Dollars ($250) for the first offense and Five Hundred Dollars ($500) for every subsequent offense.

_____ _____
MARILYN EDWARDS, County Judge DATE

_____
BECKY LEWALLEN, County Clerk

Sponsor:_____
Date of Passage:_____
Votes For:_____ Votes Against:_____
Abstention:_____ Absent:_____