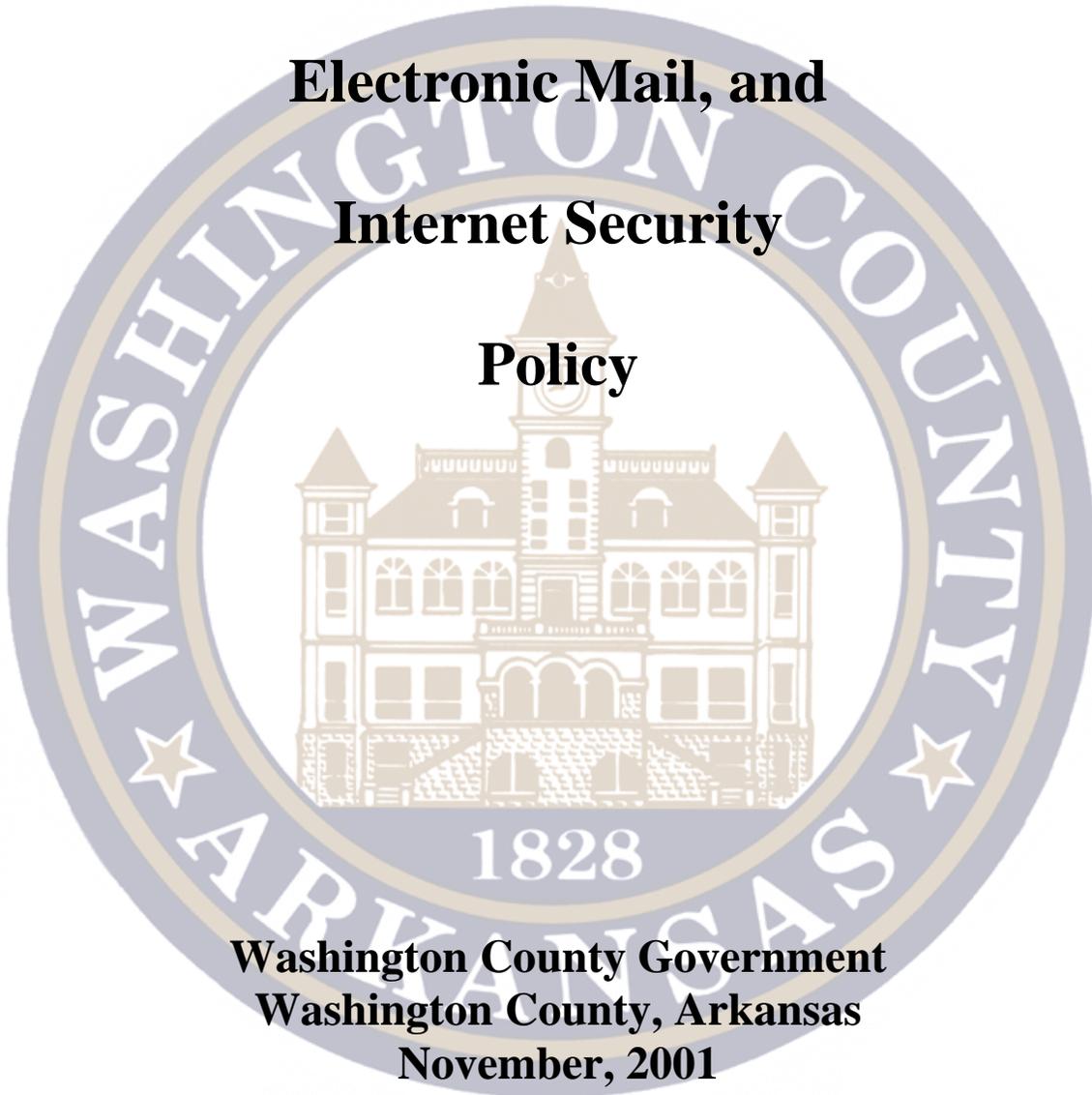


**Computer Usage,**

**Electronic Mail, and**

**Internet Security**

**Policy**



**Washington County Government  
Washington County, Arkansas  
November, 2001**

**Approved by Quorum Court 2/14/02  
Ordinance No. 2002-6**

## Table of Contents

<b>1</b>	<b>Introduction</b> .....	<b>3</b>
1.1	Purpose .....	3
<b>2</b>	<b>The Responsibility of Washington County and its Computer Users</b> .....	<b>3</b>
2.1	Opportunities and Risks .....	3
2.2	Applicability .....	3
2.3	County Property .....	3
2.4	Computer Equipment and Software Purchases .....	3
2.5	Use Without Authorization Prohibited .....	4
2.6	Authorized Usage .....	4
2.7	Default Privileges .....	4
2.8	User Accountability .....	4
2.9	Disclosing Confidential Information .....	5
2.10	Copyrights .....	5
<b>3</b>	<b>Privacy Expectations</b> .....	<b>5</b>
3.1	Respecting Privacy Rights .....	5
3.2	No Default Protection .....	5
3.3	No Guaranteed Message Privacy .....	5
3.4	The Arkansas Freedom of Information Act .....	6
3.5	Regular Message Monitoring .....	6
3.6	Incidental Disclosure .....	6
3.7	Internet Activity Logging .....	6
<b>4</b>	<b>Security</b> .....	<b>6</b>
4.1	Security Responsibilities .....	6
4.2	Problem Notification Process .....	7
<b>5</b>	<b>E-mail Policy</b> .....	<b>7</b>
5.1	Contents of Messages .....	7
5.2	Message Forwarding .....	7
5.3	User Back-Up .....	7
5.4	Purging Electronic Messages .....	8
5.5	Harassing or Offensive Materials .....	8
5.6	Paper Confirmation for Contracts .....	8
<b>6</b>	<b>Internet Policy</b> .....	<b>8</b>
6.1	Access to the Internet .....	8
6.2	Internet Content Filtering .....	9
6.3	Information Integrity .....	9
6.4	Virus Checking .....	9
6.5	Push Technology .....	9
6.6	User Anonymity .....	9
6.7	Web Page Changes .....	9
6.8	Message Interception .....	10
6.9	Appropriate Behavior .....	10
6.10	Internet Service Providers .....	10
6.11	Establishing Network Connections .....	10
<b>7</b>	<b>Computer Usage, Electronic Mail and Internet Security Policy Revisions</b> .....	<b>10</b>
7.1	County's Right to Make Revisions .....	10

## **1 Introduction**

### **1.1 Purpose**

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

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

## **2 The Responsibilities of Washington County and its Computer Users**

### **2.1 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.

### **2.2 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. Violations of this policy can lead to revocation of system privileges by the Computer Systems Administrator and/or disciplinary action up to and including termination by the responsible elected official or their designee.

### **2.3 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.

### **2.4 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.

## **2.5 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.

## **2.6 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.

## **2.7 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.**

## **2.8 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).

## **2.9 Disclosing Confidential Information**

Users must not publicly disclose confidential information via the Internet or e-mail.

## **2.10 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.

## **3 Privacy Expectations**

### **3.1 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.

### **3.2 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.

### **3.3 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.

### **3.4 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.**

### **3.5 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.**

### **3.6 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.

### **3.7 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.

## **4 Security**

### **4.1 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.

## **4.2 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.

## **5 E-mail Policy**

### **5.1 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.

### **5.2 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.

### **5.3 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.

### **5.4 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 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.

### **5.5 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.

### **5.6 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.

## **6 Internet Policy**

### **6.1 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.**

## **6.2 Internet Content Filtering**

Washington County reserves the right to block access to specific Web pages for the following reasons:

- To define and enforce access privileges
- To protect against potential legal action
- To preserve bandwidth and server space
- To manage Internet resources

## **6.3 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.

## **6.4 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.

## **6.5 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.

## **6.6 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.

## **6.7 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.

## **6.8 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.

## **6.9 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.

## **6.10 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.

## **6.11 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.

## **7 Computer Usage, Electronic Mail and Internet Security Policy Revisions**

## **7.1 County's Right to Make 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.