

⑤ City of Conway

013573

ORDINANCE NO. 0-04-59

Doc#2004- 13425

Date 7/2004

11:14 AM

Filed & Recorded in

Official Records of

Faulkner County

SHARON RIMMER

FAULKNER COUNTY CIRCUIT CLERK

Fees \$20.00

240394

am
D.C.

AN ORDINANCE AMENDING ORDINANCE NO. 0-00-55 WHICH ADOPTED AN AMENDED EMPLOYEE HANDBOOK AND PERSONNEL POLICY FOR THE CITY OF CONWAY; DECLARING AN EMERGENCY AND FOR OTHER PURPOSES.

WHEREAS, the City Council has adopted, pursuant to Ordinance No. 0-00-73, an amended handbook to be used for personnel matters for the City; and

WHEREAS, a revision of Section II, Employee Benefits, is needed for the fair and impartial implementation of personnel policies.

SECTION 1: Section I, Employment Policies, Internet and E-Mail policy shall be added as follows:

PURPOSE

The purpose of this policy is to provide employees with guidance on the proper use of city owned computers and related Electronic Messaging Devices (EMD's). The City of Conway encourages the use of Internet (including electronic mail) to provide an efficient method to exchange information within City offices, between local governmental officials and to the public. The City expects its employees to exercise discretion and utilize these tools in an efficient and professional manner.

POLICY

New technologies provide many opportunities for enhancement of productivity and effectiveness. However, these new technologies also entail the opportunity for rapid transfer and broad distribution of sensitive information that can have damaging effects on the city and employees utilizing the same. It is the policy of this city that all employees abide by these policy guidelines when using computers, the internet, voice mail and related electronic messaging devices. This policy is intended to provide guidance on appropriate usage to the employees of the City of Conway. The policy objective is to insure that city computers, the internet, e-mail and EMD's are used first and foremost to accomplish business tasks. Every employee has a responsibility to maintain and enhance the City of Conway's image, and to use these resources in a responsible, productive manner.

Definitions

Electronic Messaging Device (EMD): Electronic messaging devices include computers, electronic mail systems, voice mail systems, paging systems, electronic bulletin boards, Internet services and facsimile transmissions.

Director of Information Technology: The city employee designated with responsibility for managing all aspects of city computers, e-mail, voice mail and Electronic Messaging Devices.

Usage

Transmission of electronic messages and information on communications media provided for employees of this city are to be treated with the same degree of propriety and professionalism as official written correspondence.

The city encourages authorized and trained personnel with access to EMD's to utilize these devices whenever necessary. However, use of any of these devices

is a privilege that is subject to revocation based on breaches of this policy. To ensure compliance with this policy, telephone, computer, e-mail and internet usage may be monitored, accessed and reviewed.

City computers, internet, e-mail and EMD's are intended for conducting business of this city. Infrequent personal use may be permissible if limited in scope and frequency, if in conformance with other elements of this policy and if not connected with a profit making business enterprise or the promotion of any product, service or cause that is not approved by this City.

Prohibited Use

Viewing, downloading and/or transmitting materials that involve the use of obscene language, images, jokes, sexually explicit materials or any messages that contain defamatory, false, inaccurate, abusive, threatening, racially offensive or otherwise biased, discriminatory or illegal material; any messages that encourage the use of controlled substances, uses the system for the purpose of criminal intent or any other illegal, immoral or unethical purpose; any message that violates or infringes on the rights of any other person, including the right to privacy.

Access to any file or database unless they have a need and a right to such information. Personal identification and access codes shall not be revealed to any unauthorized source.

Download or install any software without prior approval from the Director of Information Technology.

Download or install any executable or macro file or other materials, including search bars, from the Internet or other external sources.

Violate any copyright and licensing restriction of any software.

Permit unauthorized persons to use this city's electronic mail system.

Registering Personal Electronic Mail System (Email) Accounts.

Registering city issued email addresses for non-professional or non-city related business that could affect the performance of the city's network, causes the employee to receive unsolicited emails, or requires the City to provide time and leadership to correct the problem.

Sending and/or forwarding chain letters, virus hoaxes, urban legends, etc.

Sending and/or forwarding materials that promote a product, social, religious or political cause not approved by the city.

PRIVACY and FOIA

Confidential, proprietary or sensitive information may be disseminated only to individuals with a need and right to know and where there is sufficient assurance that appropriate security of such information will be maintained.

The electronic files, including E-mail files, of City employees are potentially subject to public inspection and copying under the state Freedom of Information Act ("FOIA"), Ark. Code Ann. 25-19-101 et seq.

COPYRIGHTED MATERIAL

Users may download copyrighted material, but its use must be strictly within the agreement as posted by the author or current copyright law and should be related to City work.

IMPORTING, INSTALLING SOFTWARE/HARDWARE

Employees shall not download or install any software, hardware, or make modifications/upgrades to any EMD without prior approval from the Director of Information Technology. All installation and importing of software or programs shall be conducted under the following guidelines to ensure protection from computer viruses.

Information stored or received on a floppy disk shall be scanned for viruses prior to installation on any city computer.

External materials or applications may not be downloaded directly to any shared (network) drive.

Employees shall observe copyright and licensing restrictions of all software applications and shall not copy software from internal or external sources unless legally authorized.

Authorized employees may remove any software for which proof of licensing (original disks, original manuals and/or license) cannot be provided.

Privately owned software may be loaded on city computers with approval from the Director of Information Technology if it is necessary for business purposes and is properly licensed. Personal software will be removed if it conflicts with city hardware or software, interferes with the ability of other members to access or utilize the computer or occupies excessive storage space needed by the city.

The Director of Information Technology must authorize all hardware enhancements or additions to city owned equipment. The IT Director is responsible for determining proper installation procedures if approved.

COMPUTER ETHICS

Employees have a responsibility to conduct themselves in an ethical manner. The following information suggests some areas where ethics issues will arise and provides some suggestions on how to deal with those issues:

Data obtained inappropriately should not be used.

Finding and reporting a system weakness is not a license to take advantage of it.

Every user has a responsibility to produce acceptable work and be accountable for that work.

Organizations and individuals have rights to privacy. Where confidentiality of information is unclear, it should not be divulged.

Electronic mail should be treated as privileged in same manner as first class U.S. mail.

Use of personal information voluntarily provided, for purposes other than agreed to, is unethical.

SECURITY AND SAFETY

To avoid breaches of security, employees shall log off any personal computer that has access to the City's computer network, electronic mail, the Internet or sensitive information whenever they are away from their computer for an extended period of time or at the end of their work period. Employees shall lock their computer using the Ctrl-Alt-Del function whenever they leave their computer for a short period of time (break, copying, faxing, etc.).

Employees should keep sensitive information from being viewed by unauthorized persons while it is being displayed on a computer. Closing, obscuring the display or by locking their computer using the Ctrl-Alt-Del function.

When an employee resigns or is terminated the Director of Information Technology must be notified immediately so the employee's accounts can be closed.

AUDITS

The Director of Information Technology or authorized persons will conduct periodic audits to assure compliance with the City policy. Employee action or inaction contradictory to this policy, in part or in its entirety, may lead to disciplinary action up to and including termination.

SECTION 2: Three (3) copies of the revised section of the Amended Employee Handbook, City of Conway, Personnel Policy shall be and are hereafter kept on file in the Office of the Clerk/Treasurer.

SECTION 3: That all ordinances in conflict herewith are repealed to the extent of the conflict, specifically, Ordinance No. 0-00-55 and Ordinance No. 0-00-73.

SECTION 4: That this ordinance is necessary for the protection of the peace, health and safety of the citizens of Conway, and therefore, an emergency is declared to exist, and this ordinance shall go into effect from and after its passage and approval.

PASSED this 8th day of June, 2004.

APPROVED:



MAYOR TAB TOWNSELL

ATTEST:



MICHAEL O. GARRETT, CITY CLERK