

Fayetteville Police Department
Fayetteville, Arkansas 72702

GENERAL ORDER #16

SUBJECT: INTERNET AND E-MAIL CODE OF CONDUCT

CROSS-REFERENCE: City Policy GA-17

DATE APPROVED BY COP: July 12, 2001


Chief Richard L. Watson

PURPOSE: The Internet and electronic mail system have been provided by the City of Fayetteville Police Department for the sole purpose of improving employee productivity and efficiency in the conduct of Police Department administration. Access to the system permits employees to connect to information resources on a global basis. Each employee has a responsibility to maintain and enhance City government's public image and to use the Internet and e-mail in a productive manner consistent with this good public image. This policy governs Internet access, and the retention, disclosure and public nature of all communications created, sent or received by Police Department employees using the Police Department's system. Therefore, the following Procedures are set forth to establish the standards of conduct to be followed by each employee using the Police Department's access to the internet and the use of e-mail. The Police Department intends to enforce the specific elements of the General Order set forth below and reserves the right to make changes from time to time if technology or circumstances warrant.

ORDER: All Fayetteville Police Department Employees using the Department's Internet and/or E-Mail service must follow the Procedures listed below.

Procedures:

1. Employees accessing the Internet are representing the Police Department. All communications should be for work related reasons EXCEPT FOR APPROXIMATELY FIFTEEN MINUTES PER SHIFT BUT NEVER TO EXCEED NORMAL BREAKTIME. Employees are responsible for utilizing the Internet in an effective, ethical, and lawful manner. Internet relay chat channels may be used to conduct official Police Department business or to gain technical or analytical advice. Databases may be accessed for information as needed. E-mail may be used for business contacts.
2. If the Internet service can be provided through the Police Department's system, employees at all Police Department facilities are prohibited from accessing the Internet at that facility through a modem connected to an outside service provider

unless authorized by the Chief of Police.

3. The Police Department's Internet and e-mail system may not be used to solicit or proselytize for commercial or non-profit ventures, religious or political causes, outside organizations, or other non-job related issues such as the advancement of personal views or causes. Use of the Internet must not disrupt the operation of the Police Department's networks or the network of other users. Users must not knowingly propagate any worm, virus, Trojan horse or trap-door program code.
4. Each employee is responsible for the content of all text, audio or images that they place or send over the Internet. Fraudulent, harassing or obscene messages are prohibited.
5. All messages originating at the Police Department must have the originating employee's name attached. No messages are to be transmitted under an assumed name. Users may not attempt to obscure the origin of any message. Information published on the Internet must not violate or infringe upon the rights of others. No abusive, profane or offensive language is to be transmitted through the system unless tied directly to an investigation or approved training issue. Employees who wish to express personal opinions on the Internet are encouraged to obtain their own user names on their personal Internet System.
6. Sexually explicit material may not be displayed, archived, stored, distributed, edited or recorded using the Police Department's Internet, network or computing resources unless tied directly to an investigation or approved training issue. The display of any sexually explicit image or document is a violation of the City's policy on sexual harassment unless tied directly to an investigation or approved training issue.
7. Harassment of any kind is prohibited. Messages, unless tied directly to an investigation or approved training issue, may not be offensive or disruptive. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.
8. Software may be downloaded only for Police Department business purposes and any software obtained becomes property of the Police Department. To prevent computer viruses from being transmitted through the system, there will be no unauthorized downloading of any software. All software downloads must be authorized by the Information Services Manager and will be done by the Information Services Division. Downloaded software must be properly licensed and registered if required.

9. Copyrighted materials belonging to other entities may not be transmitted by staff on the Internet. One copy of copyrighted material may be downloaded for personal use in research. Users are not permitted to copy, transfer, rename, add or delete information or programs belonging to other users unless given express permission to do so by the copyright owner.
10. All messages created, sent or retrieved by staff over the Internet are the properties of the City, with the record and content deemed public information, which may be subject to the Arkansas FOI Act even messages created, sent or retrieved by staff that is thought to be personal. The Police Department reserves the right to access and monitor any or all messages and files on the computer system as deemed necessary and appropriate. Internet messages are public communication and are not private. An employee should not have any expectation of privacy as to his or her Internet usage while using the Police Department service. Software and systems are in place that can monitor and record all Internet and e-mail usage. All communications including text images can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.
11. All Internet downloads are strictly prohibited by individual employees. Employees must request all downloads through the Information Services Division. Employees may not use the Police Department's Internet facilities to download entertainment software, images, videos or games, or to play games against opponents over the Internet. Employees shall not download mp3 files or direct radio station feeds. The Internet is to be employed only as a business tool and must not be used to interfere with productivity.
12. The Police Department has installed an Internet firewall to assure the security of the Police Department's network. Any attempt to disable, defeat or circumvent this facility will be deemed a serious violation of policy.
13. Violations of any guidelines listed above may result in disciplinary action up to and including termination. Any illegal activity will be deemed grounds for immediate termination.
14. A fully executed copy of the authorization and use acknowledgment form (page 5 of this general order) must be submitted to the Information Services Manager prior to activating e-mail or Internet access for any employee's workstation.
15. Upon being issued authorization to use the Police Department's Internet and e-mail services, each employee will be responsible for all transmissions that occur under their authorization code. Therefore, each employee must successfully log off before leaving the computer.

16. All inappropriate e-mail or visits to an unauthorized web site during an official investigation or training exercise must be logged in the "Prohibited e-mail or web site access ledger". The Lieutenant in charge of the Detective Division will maintain this ledger. A sample page is included on page 6 of this General Order.

