UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF ARKANSAS

IN THE MATTER OF INTERNET POLICY
FOR THE EASTERN DISTRICT OF ARKANSAS

GENERAL ORDER NO. 47

The following shall be the Internet policy of this Court:

1. **PURPOSE.** The purpose of this bulletin is to provide guidance for "acceptable use" of the Internet by Court employees.

2. **SCOPE.** This bulletin applies to all Court employees who use the Internet in the performance of their jobs.

3. **RESPONSIBILITY.** With the increased use of Internet services throughout the Judiciary, it is important that these tools are used properly and in the best interests of the government. Since no two employees will use the Internet in exactly the same way, each user will have to exercise individual responsibility and judgment as to appropriate use within the broad guideline of "official business." Judicial Officers and Unit Executives are responsible for determining which of their staff require Internet access to carry out their jobs; providing required computer systems, software, and security devices; and, training on the proper use of the Internet. Copies of this Bulletin should be provided to each staff member who either has or requests Internet access.

4. **WHAT USERS SHOULD KNOW ABOUT INTERNET AND INTERNET E-MAIL.**

The Internet is an informal collection of government, military, commercial, and educational computer networks. It is essential that users understand some of the limitations of the Internet and the Internet e-mail system including security and delivery of an e-mail message.

The Internet is an **unsecured** network. As such, information and e-mail on the Internet can be read, broadcasted, or published without the knowledge or consent of the author. Users should be aware that cc:Mail is converted to e-mail and may be sent via the Internet. Consequently, cc:Mail should be treated with the same precautions as e-mail. Most sites maintain records of all users or entities accessing their resources. These records may be open to inspection and publication without the user's knowledge or consent. If the activity of the user is other than official business, the publication of that activity could prove to be an embarrassment for the Court and the entire federal Judiciary.

Internet e-mail traffic is subject to inspection by a variety of persons and mechanisms, authorized and otherwise. Authorized personnel on any node between the origin and destination of a message may have to inspect message contents in order to dispatch stalled deliveries or resolve other failures. Users should not expect the messages they send or receive via the Internet to be private. Delivery and delivery times are not guaranteed due to unpredictable intermediary system and network outages, slowdowns, and polling intervals, etc. Consequently, users should not rely on Internet e-mail for time-sensitive communications or guaranteed delivery. Some messages may not be delivered although the message was correctly addressed. Receipt or non-receipt can only be confirmed through other positive means, not by inference or assumption. **Note**: the cc:Mail "Receipt

Requested" feature may not be honored by systems on the Internet. Users should not rely on this feature for Internet e-mail.

Delivery and response times on the Internet, as well as the DCN, are determined by traffic and congestion on the network. For example, sending large files such as digital images to a large number of recipients will delay other traffic and may overload the system causing failure. Users are encouraged to use discretion when forwarding large e-mail messages to group addresses or distribution lists. Congestion on the network can be caused by the propagation of "chain letters" and "broadcasting" of lengthy messages to lists or individuals. These uses also place a burden on the shared data storage device of the e-mail post office.

Internet e-mail access grants users the ability to subscribe to a variety of e-mail news groups, list servers, and other sources of information. These services are a potentially valuable information tool for some e-mail users; but again, the potential for network congestion is high. Users should be cautioned on the widespread use of mailing lists and list servers. In general, low-volume business related lists will not be a problem.

Users should focus on one subject per message and always include a pertinent subject title for the message to enable the reader to locate the message quickly. Remember the basic elements of effective writing: clarity, brevity, and courtesy. Users should be reminded they bear sole responsibility for material they send, access, or display on the Internet or in Internet e-mail.

5. **PROCEDURES.** The following procedures should be followed to ensure that employees use the Internet safely and productively, and that the Internet is not used in any way that could compromise the interests of the judiciary. These guidelines apply to all Internet services,

including but not limited to: electronic mail (e-mail), Web browsers, Telnet, and File Transfer Protocol (FTP).

Access to Internet: Employees with a valid need to use the Internet should secure written approval of their Judicial Officer or Unit Executive by including their name, purpose of Internet access, estimated hours per month use, and that they understand that access is provided for official government purposes only. The Judicial Officer or Unit Executive should forward their approval to the Systems Department for connection. Government-provided Internet access is subject to being withdrawn at the discretion of the Judicial Officer or Unit Executive.

Monitoring: The Systems Department will not monitor the Internet activity log for compliance with acceptable use policies unless requested by a Judicial Officer or requested by a Unit Executive and approved by the Chief Judge of the district.

Responsible Internet Policies: The Internet allows employees to have electronic discussions of official government matters with other federal employees, private sector employees, and the worldwide general public. The Internet audience is virtually unlimited, and because one never knows who will read posted messages, care should be taken with what is said and how it is said. Connection to the Internet offers employees significant benefits in terms of increased access to information resources. However, connection to the Internet is a privilege and not a right.

When accessing the Internet, employees must adhere to the same code of ethics that governs all other aspects of judiciary employee activity. Internet activity should not interfere with performance of official duties. Staff are encouraged to use the Internet to accomplish job responsibilities, to become more knowledgeable about Internet capabilities, and further the Court's mission.

Each Judicial Officer or Unit Executive may permit designated staff to use the Internet on personal time. Such use provides staff with an opportunity to practice Internet skills and explore Internet resources. Our Court benefits by permitting staff to use their own time to develop these skills. In the current environment of shrinking budgets and the need for staff to take on new and greater responsibilities, and develop new areas of expertise, use of the Internet can be an important avenue for training and development of skills. Since the Court pays one flat fee for all Internet access, there is no additional cost for personal use of the Internet.

This policy allowing staff members to use the Internet on personal time is similar to our existing policy of allowing staff to use library collections and other resources on personal time and has similar benefits. Just as a staff member who takes books home, visits the library, and participates in court events learns about the institution and acquires skills to become a better employee, a staff member who makes use of the Internet on personal time enhances his or her knowledge and skills of electronic information resources and gains skills in information technology. This use also enhances job-related knowledge and skills and provides cost-effective self-training opportunities. By encouraging employees to explore the Internet, the Court builds its pool of Internet-literate staff who can then guide and encourage those around them. With this in mind, staff is encouraged to use official time to attend meetings and programs related to the Internet and to serve as trainers for other staff who may wish to use the Internet.

Employees may not use the Internet for prohibited activities. Employees are expressly forbidden from creating unauthorized satellite home pages or other similar works and are cautioned to use great care that no statements are made which may appear to express agency policy or position which are not authorized. Prohibited activities are:

1. making unauthorized statements regarding agency policies or practices;
2. transmitting confidential information (such as that relating to ongoing investigations, procurements, or litigation);
3. making unauthorized commitments or promises that might be perceived as binding the government;
4. using subscription accounts or commercial services that are not expressly authorized;
5. posting an unauthorized home page or similar web site;
6. engaging in chat room discussions through e-mail, etc.;
7. sending or displaying messages or pictures that are of an obscene or sexually explicit nature as defined in Miller v. California 413 U.S. 15, 23 (1972) or Ark. Code Ann. (1987) §5-68-302(4) ;
8. using the network connection for commercial purposes or private gain;
9. using the network for illegal activities;
10. unauthorized personal use.
11. Improper use or distribution of information is also prohibited. This includes copyright violations such as software piracy (Copyright law protects software authors and publishers just as patent law protects inventors. The Court may incur a legal liability for unauthorized copying of files or software even if the copy is used for official business).

Employees should show respect for intellectual property and creativity by giving appropriate credit when files or portions of files are used while carrying out official duties. Employees should be mindful of procurement sensitive information and should not transmit it over the Internet.

Judicial Officers, of course, occupy a special position in our system, which position necessitates that they enjoy the utmost autonomy. This means, by necessity, their Internet access must be protected by complete confidentiality, as with their research on Westlaw and Lexis. In order to protect the confidentiality of Internet research by Judicial Officers, no monitoring of judges' Internet activity shall be attempted by any court employee. Any violation of their rule shall result in immediate termination from employment.

It is SO ORDERED this 28th day of May, 1997.

/s/ Stephen M. Reasoner
STEPHEN M. REASONER, CHIEF JUDGE
UNITED STATES DISTRICT COURT