SUPERIOR COURT OF THE DISTRICT OF COLUMBIA

ADMINISTRATIVE ORDER 01-08

Attached are the Internet Polices and Procedures for the Superior Court of the District of Columbia. By this order these policies and procedures are made the official internet policies and procedures of the Court, governing the use of the internet by any judicial and non-judicial court employee.

BY THE COURT
April __5___, 2001

_____/S/_____
Rufus King, III
Chief Judge

Copies to:

All Judges
Hearing Commissioners
Executive Officer
Clerk of the Court
Division Directors
Director, CCAN Office
Director, Public Defender Service
Librarian

SUPERIOR COURT OF THE DISTRICT OF COLUMBIA

INTERNET POLICIES AND PROCEDURES

I. GOAL

The efficient utilization of the Internet for communication and research can improve the quality, productivity, and cost effectiveness of the Superior Court of the District of Columbia workforce. While it is a fascinating and powerful tool, the Internet can also be a potential threat to the security and integrity of an organization's network resources and data. The goal of this policy is to ensure the proper use of this resource and to govern behavior pertaining to access and usage of publicly accessible computer networks such as the Internet. The procedures and principles presented in this policy apply to all Superior Court of the District of Columbia personnel, volunteers and other affiliates, hereafter known as "User", who use Court-provided publicly accessible computer networks such as the Internet, regardless of the User's location when accessing the network.

These policies and procedures concern Internet browsing and E-Mail only. The overall, guiding principle is that the Court is providing Users with a business tool to assist them in the performance of their official duties.

II. INTERNET BROWSING

This function includes using the Court's Internet accounts, browser software, computers, phone lines and/or modems to provide a gateway into the worldwide web of *other* Internet service provider (ISP) resources. Once connected, the browsing process itself includes entering web site addresses, "clicking on" links to other web pages and using search engines to locate and peruse Internet web sites.

Browsing is often "interactive," with data or information sent from the web site to the User and vice-versa. This is usually a function initiated by the User (sending a name or E-Mail address, downloading a file/picture, etc.), but also can be quite unknown to the User (Internet cookies, etc.). As such, browsing can be potentially harmful to the Court by introducing virus-infected files to the network. Browsing also subjects the User to the possibility of receiving a deluge of unwanted material such as targeted marketing and "junk" mail.

For its own protection, the Court has employed a "firewall" and other such technologies that can prevent certain file transfers, limit access to certain web sites and ***track all User browsing activities.*** This information can be used to determine compliance with these policies and the appropriateness of the browsing activity.

Users requiring browsing access to the Internet must obtain written permission from the Executive Officer and provide detailed justification for the browsing activity. This written permission is to be forwarded to the Information Technology Division which will assign Internet access by configuring User hardware and assigning IDs/passwords.

III. INTERNET E-MAIL

The Court can furnish a User with an Internet E-Mail address and mailbox which can be accessed world-wide on the Internet to send and receive messages. It is an excellent tool for communicating short messages to associates and colleagues across the country. Documents stored on the User's computer can be "attached" to these messages and sent to others.

All E-Mail material is subject to audit by the Court and can be illegally intercepted by others during transmission on the Internet.

Besides the common danger of receiving virus-infected files, problems can arise from incompatible software versions and excessive document length.

An Internet E-mail address will be assigned by the Information Technology Division upon approval of the Executive Officer, once the proper hardware, software and network connections have been installed. This E-mail address is for E-mail purposes only and will not provide the User with browser-based capability on the Internet.

IV. COMPLIANCE

Each User will be required to sign a release, which will be kept on file by the Information Technology Division, acknowledging that this policy and procedures document has been read and understood.

The responsibility for ensuring compliance with these policies and procedures lies with the User's immediate supervisor/manager and ultimately the Executive Officer. Failure to comply with these policies and procedures can lead to the revocation of system privileges and/or disciplinary action.

V. SPECIFIC POLICIES

A. Internet E-mail and browser access are to be used for official Court business. Employees may use the E-mail for brief, personal communication with family, friends or associates, as they would the office telephone.

B. All communication via the Internet shall be conducted in a professional manner and consistent with the same standards as formal letters.

C. Files downloaded from the Internet must be scanned for viruses.

D. Users must not place Court software, internal memos, or other information on any publicly accessible Internet computer, unless the posting of these materials has first been approved by the Executive Officer.

E. Users are prohibited from accessing, downloading, or exchanging pirated software, games, purloined passwords, or any other inappropriate material. No executable software (programs that 'run' on the computer, as opposed to files) will be installed on the Court's computers without the approval and assistance of the Information Technology Division. This includes browsers, screen savers, personal schedulers, "free" access to other ISPs, and the like.

F. The Superior Court of the District of Columbia strictly adheres to license agreements of all software vendors. When at work or when Court networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Similarly, reproduction of work posted or otherwise available over the Internet must be done only with the permission of the author/owner.

G. Non-public record information must not be sent over the Internet unless it has first been encrypted in a manner approved by the Information Technology Division.

H. Users will not subscribe to any list servers or mailing list without approval from the appropriate Court official.

I. Any use of the Court's Internet E-mail or browser which may result in a financial or other obligation upon the Court must be approved in advance by the Executive Officer.

J. At any time and without prior notice, the Court reserves the right to examine E-mail, personal file directories, and other information stored on Court computers. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of Court information systems.

VI. EMPLOYEE AGREEMENT

By signing this document you agree to adhere to all policies and procedures set forth in this document.

_____ _____
Employee Name (Please Print) Date

_____
Employee Signature

E-Mail Address Requested ☐ Yes ☐ No

Browser Access Requested ☐ Yes ☐ No

_____
Executive Officer Approval

(Please Attach Justification)