

IN THE CIRCUIT COURT OF THE FIFTEENTH JUDICIAL CIRCUIT
IN AND FOR PALM BEACH COUNTY, FLORIDA

ADMINISTRATIVE ORDER NO. 11.704 9/08*

IN RE: POLICIES FOR USE OF
PERSONAL COMPUTERS BY
JUDGES AND COURT PERSONNEL

All judges and court personnel in the Fifteenth Judicial Circuit have been furnished or have access to personal computers ("PC's") to assist them in their work-related functions and assignments. **There is a recognized need to promulgate uniform policies to ensure the safety of the network and compliance with state and federal licensing and intellectual property laws.**

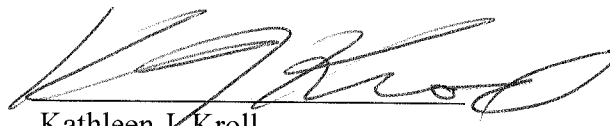
NOW, THEREFORE, pursuant to the authority conferred by Florida Rule of Judicial Administration 2.215, it is **ORDERED** as follows:

1. **The Court's computer systems (including the Court's computer equipment, software, e-mail system and Internet access) may be used only for a purpose that is court- or law-related, or that involves other legitimate matters.**
2. **Using the Court's computer system for the purposes of any employment outside the State Court's System or for private commercial or business purposes is prohibited.**
3. To ensure safe and effective computing with the Court's networked systems:
 - a. Application settings, operating system software settings, or network configuration settings of your machine are not to be changed as each workstation has been configured to ensure safe and effective computing with the Court's networked systems.
 - b. Material from unknown web sites, additional software, or upgrades to existing standard court software should not be downloaded or transferred to a court computer as it can result in software incompatibilities, destruction of data, or licensing violations. Changes to the workstation should only be made by the systems administrators.
 - c. Peer-to-peer software (e.g., Kazaa, Napster, WinMX) should not be downloaded on any court computer system. The use of peer-to-peer applications consumes large

amounts of network resources and exposes the computer and the Court network to viruses, worms, spyware, and other security threats.

4. **All state and county employees who work in the court system shall comply with the Computer Use Policy that is to be signed by all employees and which is retained in the employee's personnel file. A copy of the Computer Use Policy is attached as Exhibit "A".**
5. **Definitions:**
 - a. **"Court-related" means that the purpose furthers legitimate interests of the courts.**
 - b. **"Law-related" means that the purpose promotes a better understanding of the law and legal trends.**
 - c. **"Other legitimate matters" are activities relevant to users' personal life or family that do not detract from the Court's dignity or routine functions, and that do not interfere with the timely performance of the normal work duties.**

DONE and SIGNED in Chambers, in West Palm Beach, Palm Beach County, Florida,
this 29 day of September, 2008.



Kathleen J. Kroll
Chief Judge

*supersedes admin. order 2.045-4/97

EXHIBIT "A"

THE FIFTEENTH JUDICIAL CIRCUIT COMPUTER USE POLICY

I. ACCEPTABLE USE

The security of the Fifteenth Judicial Circuit's ("Court") data and systems is a top priority. The Court's systems administrators and Palm Beach County's ISS department go to great lengths to ensure that our software and systems are as secure as possible in order to reduce the risks of virus attacks, compromise of the network systems and services, and legal issues. To make our computing environment as safe as possible, your systems administrators are directed to ensure that the following policies are followed.

1. Employees and judges using the Court's computer systems (including the Court's computer equipment, software, e-mail system and Internet access) may do so only for a purpose that is court- or law-related, or that involves other legitimate matters. "Court-related" means that the purpose furthers legitimate interests of the courts. "Law-related" means that the purpose promotes a better understanding of the law and legal trends. "Other legitimate matters" are activities relevant to users' personal life or family that do not detract from the Court's dignity or routine functions, and that do not interfere with the timely performance of the normal work duties. Using the Court's computer system for the purposes of any employment outside the State Courts System or for private commercial or business purposes is prohibited.
2. The Court is the owner of the computer systems and has the right to access, monitor, inspect, and disclose, for legitimate Court business reasons, all information and materials entered, created, transmitted, accessed, received or stored on the systems. The Court's right to access, monitor, inspect and disclose extends to all aspects of the computer systems, including Internet use and e-mail. Users of the Court's computer systems have no reasonable expectation of privacy in information and materials entered, created, transmitted, accessed, received or stored on the Court's computer systems.
3. Unique, unnecessary software, configuration settings (desktop wallpaper) and personal files are not supported and may be lost with little or no advanced notice. The Court's computing needs are fulfilled through the use of a standardized and periodically updated workstation configuration. In the event of a workstation failure or when extensive software upgrades are necessary, your workstation may need to be "rebuilt" using the standard configuration. In such cases, it is the user's responsibility to restore settings and data that are not court or law-related.
4. To ensure safe and effective computing with the Court's networked systems:
 - a. Do not change the application settings, operating system software settings, or network configuration settings of your machine. Your workstation has been

configured to ensure safe and effective computing with the Court's networked systems.

- b. Never download material from unknown web sites, install additional software, or upgrade existing standard court software. This includes software obtained via the Internet, e-mail, CD-ROM or diskette. Doing so can result in software incompatibilities, destruction of data, licensing violations or worse. Changes to the workstation should only be made by the systems administrators.
 - c. Do not download or install peer-to-peer software (e.g., Kazaa, Napster, WinMX) on any court computer system. The use of peer-to-peer applications consumes large amounts of network resources and exposes your computer and the Court network to viruses, worms, spyware, and other security threats. Use of this type of application could expose you and the Court to legal liability for the distribution of pirated computer software, copyrighted music and movies, etc.
- 5. Always "lock" your workstation before leaving it unattended and do not attempt to modify screen-saver settings. All workstations should be set to a default screen-saver that will automatically "lock" the workstation after being left idle for 30 minutes. If you leave your workstation before the screen-saver has engaged, you should lock your workstation manually by pressing the windows and the "L" key.
- 6. Do not share your password or account with anyone. Authorized users are responsible for the security of their passwords and accounts.
- 7. Save all work-related files in the proper location as outlined below. Data that is lost due to a system failure or other unplanned event cannot be recovered unless it is stored in the appropriate location; nor can the confidentiality and integrity of files be guaranteed if they are not stored in the appropriate location. It is a good practice to save your work frequently.
- 8. With any system, storage capacity is neither limitless nor free. Therefore, we all must cooperate to avoid intentional or unintentional "abuse" of network resources. In this regard, it is important to recognize that inappropriate utilization of network storage capacity by just a few end-users can, and may, result in insufficient storage capacity for all. Activities that are not work-related are particularly noteworthy from the standpoint of file storage. Typical examples of files that are not work-related are nonstandard screen-savers, graphics (including photos), files, music, e-mail, CD-ROM or diskette. The problem with such items is that they are generally large and consume an inordinate amount of system storage capacity. In this regard, you may have a Personal folder on your workstation identified as "Personal" to store files that are: a) not work-related and b) qualify as "other legitimate matters" as per this policy regarding acceptable use. Items stored here will be your responsibility to maintain and may be subject to loss in the event of a system failure.
- 9. All hosts used by judges and employees (e.g., laptops, tablet pc, home computers) that are connected to the court network via ethernet cable, wireless, dial-up, or VPN, shall be

continually executing approved virus-scanning software with a current virus database, and the operating system shall be patched with the most current service packs, patches, and/or hotfixes as recommended by your systems administrator. There will be mandatory routine maintenance for all court-owned portable computing devices.

10. Upon leaving work at the end of the day, save your work, exit from any open applications, and restart your computer (this will leave your computer in a locked state). Several maintenance tasks are performed on the Court's systems after working hours but may fail to occur if your computer is turned off at night. Some of the tasks may cause loss of data if you have not saved your work in progress and closed open applications.
11. Court users should adhere to these policies at all times. Compliance with the terms of the Court's Computer Use Policies is a condition of employment. Violation of the policies may subject users to disciplinary action, up to and including dismissal. If you have any questions or concerns regarding these policies, please feel free to contact your systems administrator.

II. PASSWORDS

12. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the network. All judges and employees are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.
13. Court-related (i.e., Windows workstation/e-mail, VPN account, CMS, etc.) passwords should never be written down or stored on-line. Try to create strong passwords that you can easily remember, but would be hard for someone else to guess.
14. There is no need to share passwords in order to share work documents. If you are out of the office and another court employee or judge needs access to a work document that you have stored in your network folder, upon approval by the supervisor, the systems administrator can assist with this request.
15. If an account or password is suspected to have been compromised, contact your systems administrator immediately.

III. E-MAIL*

16. **Appropriate Use of E-mail** - The Court's e-mail system provides a valuable communication link and should be used for court-related, law-related or other legitimate purposes as outlined in Section I. E-mail messages go out under the Court's address, which is essentially the Court's "electronic letterhead." Thus, e-mail should not include any information that would reflect poorly on the Court (e.g., "off-color" comments, insensitive jokes, racial slurs) or that may be construed as representing the opinion/policy of the Court proper. Do not forward e-mail reports about computer viruses, profit-making schemes, or "chain letters." Users' e-

mail can be retrieved and may be disclosed in response to a subpoena or court order, or an investigation concerning misconduct. Global e-mails (for example, e-mails addressed to SC-Everyone, OSCA-Everyone) or mass e-mails (e-mails sent to multiple users) should only be sent for official court business. Global and mass e-mails may not be used for non-court sponsored solicitations, such as advertising the sale of personal property, fundraising activities, and communications promoting political positions or actions.

17. **Accessing the Court's E-mail System via the Web** - When accessing webmail, do not configure the login to remember your password. Do not leave the computer device without logging out of webmail and closing the Internet Explorer page.
18. **Accessing Outside E-mail** - Accessing web-based e-mail accounts (such as HotMail, YahooMail, NetscapeMail, etc.) while at work is strongly discouraged but will be permitted during break periods. If you must do so for court-related, law-related or other legitimate purposes, consult your systems administrator regarding the service you must use and the appropriate use of that service. More importantly, do not open or download e-mail attachments from a web-based e-mail account.
19. **Suspicious or Questionable E-mail** - It is not uncommon for false virus warnings, known as "hoaxes" to be inappropriately sent in mass via e-mail by mal-intentioned individuals on the Internet. Forwarding hoaxes to others puts undue strain on the Court's systems and can create unnecessary confusion or even panic. If you receive an e-mail that is suspicious, unsolicited, appears to be a spoof or a hoax, or contains a warning, immediately contact your systems administrator. Do not open the e-mail and do not forward the e-mail to anyone.
20. **Attachment Blocking** - Certain e-mail file attachments that are commonly used to spread viruses may be blocked from entering our e-mail system. If you are not able to receive a court or law related e-mail attachment because it is being blocked, please contact your systems administrator for assistance.
21. **Attachment Size Limitations** - There is a size limit on e-mail attachments coming into and leaving our e-mail system. This limit protects our e-mail system from unnecessary strain. If you are not able to send or receive a court or law related e-mail attachment, please contact your system administrator who can assist you with other options for transferring files. We have no control over the attachment size limits that other entities enforce.
22. **E-mail and Public Records Requirements** - All records made or received in connection with the transaction of official business by the Court are public records. These records must be retained for specified amounts of time, and are subject to public disclosure, upon request. Public record e-mails are transitory if they are created merely for communication of information, rather than to perpetuate knowledge. Transitory e-mails do not set policy, establish guidelines or procedures, certify a transaction, or become a receipt. Transitory e-mails include those that involve only short-lived administrative matters, such as scheduling meetings, suggesting revisions to a document that has yet to be finalized, or requesting supplies. A transitory e-mail can be deleted once it is obsolete, or superseded by other

records. E-mails concerning only personal matters are not public record unless the volume of personal emails can be viewed as interfering with or affecting job performance.

23. **E-mail Retention** - All e-mail transmitted on the Court's e-mail system will be archived for the purpose of complying with the retention requirements as provided for in the Florida Rules of Judicial Administration. Employees should be aware that all e-mail will be archived and maintained indefinitely.

IV. HARASSMENT

24. The Fifteenth Judicial Circuit's policy is to provide a safe and comfortable workplace for all employees. This includes freedom from harassment based on race, religion, sex, national origin, age or disability. Sending any offensive messages by means of the Court's computer or E-mail system will not be tolerated. Failure to comply with this policy may result in discipline up to and including dismissal.
25. Should you receive any improper messages via E-mail or over the Internet at your work email address or work computer, you should immediately report the situation to your supervisor. Should you receive any improper messages via E-mail or over the Internet at your personal email account or personal computer from a co-worker or supervisor, you should immediately report the situation to your supervisor. If for any reason you are unable to advise your supervisor, bring the matter to the attention of the Trial Court Administrator or the Human Resource Manager. The Trial Court Administrator and/or Human Resource personnel will investigate any reported instances of misuse of the Court's computer system or unwanted and improper electronic communications from co-workers or supervisors. Failure to report the dissemination of offensive material may result in disciplinary action.

V. APPLICABILITY

26. This policy applies to all State employees and to all County-funded Court employees.

EMPLOYEE ACKNOWLEDGEMENT AND CONSENT

I acknowledge that I have read and understand the Court's Computer Use Policies. I understand that the Court and/or Palm Beach County is the owner of the Court's computer systems, and has the right to access, monitor, inspect and disclose, for legitimate Court business reasons, information and materials contained or stored on the computer systems. I understand that the Court's right to access, monitor, inspect and disclose extends to information and materials concerning users' Internet use and e-mail. I understand that adherence to the computer use policies is required as a condition of employment, and I consent to the terms of the policies.

Employee Signature

Employee Printed Name

Date

*includes Instant Messenger where applicable

Exhibit "A"