

IN THE EIGHTH JUDICIAL CIRCUIT OF FLORIDA
ADMINISTRATIVE ORDER NO. 8.611

ACCEPTABLE COMPUTER USE POLICIES

WHEREAS, the Chief Justice of the Florida Supreme Court has recommended that each circuit adopt a computer use policy; and

WHEREAS, judges, judicial assistants, externs, volunteers, and court staff have been furnished or have access to computers to assist them in their work-related functions and assignments; and

WHEREAS, it is necessary to establish uniform policies within the Eighth Judicial Circuit, to ensure the efficient and responsible use of computers by all users; and

WHEREAS, it is essential to protect the security of the Court's data and computer systems.

THEREFORE, it is hereby

ORDERED that the following computer use policies are adopted and shall apply to all users of the Court's computer systems.

1. You may use your computer for Court and law-related matters and for personal (non-commercial) reasons that do not detract from the Court's dignity and operations, and that do not interfere with the timely performance of work duties. **Users are expected to demonstrate a sense of responsibility and not abuse this privilege.**
2. Don't use the computer for private commercial or business enterprises.
3. Don't change application settings, Windows OS settings, or network configuration settings.
4. Don't download material from unknown websites, install additional software, or upgrade existing standard court software.
5. Don't install peer-to-peer software (e.g. Kazaa, Napster, BitTorrent), listen to streaming audio (aka "Internet Radio") or view streaming video (such as YouTube, Google Video,

- and the like). It's permissible to view streaming video of work-related material (County Commission meetings or Supreme Court video feeds, for example.)
6. Don't download large files from the Internet or from another county during business hours. If you need to download a large file, contact Court Technology to see if you can do so after 5:00 p.m., or even during lunch hour if the file is critically needed.
 7. **Don't share your password with anyone.**
 8. Don't send e-mail from your court account that reflects poorly on the Court, or could be construed as representing the opinion or policy of the Court.
 9. Don't forward e-mail reports about computer viruses, profit-making schemes, or chain letters.
 10. Don't forward e-mail containing "humorous" video and audio files (including Shockwave Flash animation files [files with an .swf extension]).
 11. Don't send non-court-business e-mail to our Court e-mail lists, such as "All Judges" or "All State Employees".
 12. Don't set your web browser to remember passwords when accessing court e-mail or other court websites.
 13. Don't bring your home computer into the office and connect it to the network.
 14. Be aware that our Internet connections are provided by the State Supreme Court & the counties of our circuit; as such, a user's web browsing activity **could be monitored and logged. Don't access inappropriate websites.**
 15. **Be aware that all records made or received in connection with the transaction of official business by the 8th Judicial Circuit are public records.** These records are subject to public disclosure upon request. Certain transitory e-mails and personal e-mails are exempt from the disclosure requirements. All e-mail sent or received on your Court e-mail account will be retained by the system via tape backup and archiving indefinitely, even when deleted by the user.
 16. Do not make changes to Wikipedia, MySpace, Facebook or any non-work-related web site visible to the public. Third parties (including the media) can track & publicize this activity.

17. Unique, unnecessary software, desktop wallpapers, and personal files stored on local hard drives may be lost at any time. It's the user's responsibility to restore settings and data that aren't Court or law related.
18. "Lock" your workstation before leaving it unattended, or leaving for the day. (press Ctrl-Alt-Delete, then press Enter or click on "Lock Computer"). Your workstation should be set to automatically lock itself after 30 minutes.
19. Leave your computer on overnight so system updates can be applied.
20. Save your work in your "My Documents" folder or the S: drive; non-work-related files (in accordance with section 1) should be saved in a "Personal" sub-folder in "My Documents".
21. Have virus-scanning & all software updates applied on any home computer that connects to the Court network via dial-up or VPN.
22. Use good passwords for all accounts. A good password is at least seven characters long, contains UPPER and lowercase letters, and at least one number. It should not be based on a word in any dictionary, or any personal information (name of a spouse, or pets, phone number, etc.) It shouldn't be easily guessable by anyone, and as stated above, **should not be shared with anyone.**
23. Arrange with Court Technology to create shared folders on the S: drive so you and other employees may work on files together **without sharing passwords.**

ORDERED on 3 ~~December, 2007~~ January 2008.


Frederick D. Smith, Chief Judge