

**UNITED STATES DISTRICT COURT
UNITED STATES PROBATION OFFICE
SOUTHERN DISTRICT OF INDIANA**

**POLICY REGARDING USE OF GOVERNMENT OFFICE EQUIPMENT
~ CONDITIONS, RULES, AND ACCEPTABLE USE AGREEMENT ~**

OVERVIEW

The United States District Court and the United States Probation Office for the Southern District of Indiana use computer technology in many ways. This technology allows Court staff and users to access information sources from distant locations and communicate with individuals or groups. With this opportunity comes great responsibility to ensure that Court resources and records are used appropriately.

BACKGROUND

Government office equipment, including information technology, is for the use of judiciary employees in their performance of official government business.

The judiciary, like the government's executive branch, recognizes that equipment supplied to carry out government business offers many conveniences that may be used by employees for personal needs at minimal or no additional cost to the taxpayer. This use may enable such employees to be more efficient and productive in their professional as well as their personal lives. Thus, on balance, the limited personal use of such equipment, as further described herein, is in the best interest of the judiciary.

GENERAL POLICY

Judiciary employees are permitted limited use of government office equipment for personal needs if such use does not interfere with official business and involves minimal additional expense to the government. The limited personal use of government office equipment should only occur during employees' non-work time. This privilege to use government office equipment for non-government purposes may be revoked or limited at any time by the Judges or the Clerk of Court.

The Court, acting through the Judges, the Clerk of Court or the Chief Probation Officer, may impose or maintain a more restrictive policy for personal use of government office equipment by their employees and other on-site personnel.

Internet use may be subject to time limits.

This policy does not affect employees' use of government office equipment for official business.

This policy also applies to contractor personnel, temporary employees, interns, and other nongovernment employees utilizing Judiciary office equipment.

DEFINITIONS

Privilege means, for the purpose of this policy, that the judiciary is extending the opportunity to employees for limited personal use of government office equipment in an effort to establish a work environment more conducive to efficiency and productivity. This policy does not create any right to use government office equipment for other than official government business. Nor does the privilege extend to modifying such equipment, including loading personal software or making configuration changes.

Government office equipment includes, but is not limited to, personal computers and related peripheral equipment and software, library resources, telephones, facsimile machines, photocopiers, office supplies, Internet connectivity, access to Internet services, and e-mail. This list is provided to show examples of office equipment intended to be covered by this policy, and it is not meant to be comprehensive.

Minimal additional expense means personal use that will result in no more than normal wear and tear or the use of small amounts of electricity, ink, toner, or paper. Examples of such minimal additional expenses include making a limited number of photocopies, using a computer printer to print a limited number of pages, making occasional phone calls in accordance with judiciary policy (Guide to Judiciary Policies and Procedures, Vol. XIII, Ch. XV, D.1.f.), infrequently sending e-mail messages, and limited use of the Internet.

Employee non-work time means time when employees are not otherwise expected to be addressing official business, such as off-duty hours before or after a workday, lunch periods or other authorized breaks, or weekends or holidays. Personal use means activity conducted by employees for purposes other than official government business.

GUIDANCE

Judiciary employees are specifically prohibited from using government equipment in furtherance of a private business. However, employees may, for example, use government office equipment to review Thrift Savings Plans or other personal investments; to monitor medical, dependent, or commuter reimbursement accounts; to seek employment; or to communicate with volunteer charity organizations.

In using government office equipment for limited personal purposes, employees must, at all times, avoid giving the impression that they are acting in an official capacity. If

there is a potential that such limited personal use could be interpreted to represent official business of the judiciary, an adequate disclaimer must be used, such as, "The contents of this message are personal and do not reflect any position of the judiciary or the court."

The Standards of Conduct for Judiciary Employees apply to this privilege, including the stricture that judiciary employees shall not lend the prestige of their offices to advance or appear to advance the private interests of others.

INAPPROPRIATE PERSONAL USE

Inappropriate personal use of government office equipment includes:

1. any personal use that could cause congestion, delay, or disruption of service to any government system. Examples include, but are not limited to, use of greeting cards, video, sound or other large file attachments, "push" technology on the Internet, and other continuous data stream uses;
2. the use of peer-to-peer file sharing (using programs such as Grokster, Morpheus, and certain interactive Internet games), chat rooms, and instant messaging for communicating with persons or entities outside the judiciary's private data communications network (these programs pose extraordinary security risks to the judiciary's information technology infrastructure and their use is prohibited);
3. attempting to gain unauthorized access to other systems;
4. creating, copying, transmitting, or retransmitting chain letters or other unauthorized mass mailings, regardless of subject matter;
5. using equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public, such as hate speech, or material that ridicules others on the basis of race, creed, religion, color, gender, disability, national origin, or sexual orientation;
6. creating, downloading, viewing, storing, copying, transmitting, or retransmitting sexually explicit or sexually oriented material;
7. creating, downloading, viewing, storing, copying, transmitting, or retransmitting material related to illegal gambling, illegal weapons, terrorist activities, and any other illegal or prohibited activities;
8. using equipment for commercial activities or in support of commercial activities or in support of outside employment or business activity, such as consulting for pay, administering business transactions, or selling goods or services;

9. using equipment for fund-raising activity (other than activities associated with the Combined Federal Campaign), endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity;
10. posting judiciary information to external news groups, bulletin boards, or other public sites without authority, including any use that could create the perception that the communication was made in an official capacity as a judiciary employee, and posting public statements at variance with the judiciary mission or position;
11. using equipment in a manner that results in loss of productivity, interference with official duties, or greater than minimal additional expense to the government; and
12. acquiring, using, reproducing, transmitting, or distributing without authorization any controlled information. Controlled information includes proprietary data subject to the intellectual property rights of others, such as copyright, trademark or other rights (beyond fair use), as well as computer software and data, *e.g.*, export controlled software or data.

MONITORING

The Court, acting through the Judges, the Clerk of Court or the Chief Probation Officer, reserves the right to review any material on user accounts and to monitor fileserver space to ensure appropriate use of automation resources. Such monitoring may be conducted without the knowledge or consent of individual users. However, no computer files of individual Judges or Magistrate Judges will be accessed without prior knowledge or permission of that Judge or Magistrate Judge. Unit Executives' files will be accessed without prior knowledge or permission only on approval of the Chief Judge. Exceptions may be permitted for purposes of a formal investigation by law enforcement officials or by the Seventh Circuit Judicial Council prompted by alleged criminal or ethical violations.

All persons utilizing or accessing the Court's computer system expressly consent to this monitoring.

The Clerk of the Court is delegated the authority to promulgate standards for appropriate use by the staff of the Clerk's Office. Each Judge will determine what constitutes appropriate use by that Judge's staff.

SECURITY

Computer and network security is vitally important to the Court's effective operation. Court staff may not share their passwords with persons other than their supervisor or Systems Department staff.

All passwords should be protected to enhance the security of the Court's computer system. For instance, users should not leave their passwords in locations where the passwords could be easily discovered.

Computers which are in an open or accessible area should be protected with a screen saver password when the computer is not in use, or it should be powered down when the employee steps away.

If a user discovers a computer security problem, the user should report it immediately to a member of the Systems Administration staff. The problem should be kept confidential and revealed only to the user's supervisor, Judge and appropriate Systems Administration staff.

Unauthorized attempts to logon to the Court's computer system by or posing as a system administrator or other user may result in immediate cancellation of user privileges and/or other disciplinary action. Any user identified as a security risk may be denied access to the Court's computer system.

Users may not install or cause to be installed any software without the express permission of a member of the Systems Administration staff. Also, users may not dismantle authorized software without the express permission of a member of the Systems Administration staff.

Users may not send or cause to be sent, e-mail messages which could harm the security of the Court's computer system. Access to personal Internet e-mail accounts (including AOL Mail, Gmail, Hotmail, and Yahoo! Mail) from within the judiciary's networks is discouraged. Use of these accounts poses threats to the judiciary's information technology infrastructure. For those who find this access necessary, steps to reduce the risk should be followed (see AO memo of 2/21/2006 Re: Computer Security Policies at http://jnet.ao.dcn/Memos/2006_Archive/Dir6018.html).

Vandalism of the Court's computer system will result in immediate cancellation of user privileges. Vandalism includes, but is not limited to, any malicious, intentional attempt to harm, modify, or destroy data of another user and misuse of the Internet, DCN, or other networks which are connected to the Court's network. For example, vandalism would include the uploading or creation or intentional transmission of computer viruses.

SANCTIONS FOR MISUSE

Unauthorized or improper use of government office equipment may result in loss of the privilege, limitation of the privilege, disciplinary or adverse actions up to and including termination, criminal penalties, and/or financial responsibility for the costs of improper use.

ACCEPTANCE OF TERMS AND CONDITIONS

All terms and conditions set forth above are applicable to all users of the Court's computer system unless specifically exempted by this policy, by applicable law, or by permission of the Chief Judge. These terms and conditions reflect the entire agreement of the parties and supersede all prior oral or written agreements and understandings of the parties. These terms and conditions shall be governed and interpreted in accordance with the laws of the State of Indiana and the United States of America.

I understand and agree to abide by this policy. I understand that any violation of this policy may constitute grounds for discipline and/or a criminal prosecution. I understand that should I commit a violation or knowingly assist in the violation of this policy by another person my access privileges may be restricted or revoked or other disciplinary action may be taken against me.

User Signature Date

Printed Name

Signature of Unit Executive or Designee Date