# The United States District Court
# Eastern District of Missouri

## Personal Use of Government Office Equipment

## and Computer Security

## Guidelines

Updated : December 6, 2016

## Definitions ( Guide to Judiciary Policy, Volume 15: Information Technology Ch 5: Managing IT Resources § 525.30 Definitions )

***Privilege*** means, for 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, printers, and related peripheral equipment and software,
- tablet devices and related applications,
- library resources,
- telephones,
- facsimile machines,
- photocopiers,
- office supplies,
- cellular phones, smart phones, and hands-free devices,
- internet connectivity, and
- email.

This list is provided to show examples of office equipment intended to be covered by this policy, and 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,
- infrequently sending email 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, and
- weekends or holidays.

***Personal use*** means activity conducted by employees for purposes other than official government business and that is not deemed inappropriate personal use per § 525.50.

## Guidance

Judiciary employees are specifically prohibited from using government-owned equipment in furtherance of a private business. However, employees may, for example, use government-owned equipment to:

- review Thrift Savings Plan accounts,
- monitor medical and dependent care, or commuter benefit reimbursement accounts,
- seek employment, or
- communicate with volunteer charity organizations.

## Background

This sets forth and establishes judiciary policy for employees on the appropriate use of government office equipment (including information technology) found in section **Guide to Judiciary Policy, Volume 15: Information Technology, Ch 5: Managing IT Resources § 525 Personal Use of Government-Owned Office Equipment and Resources.**

Government office equipment 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 appropriate court unit officials.

Court unit officials may apply this policy to contractor personnel, interns, and other non-government employees through incorporation by reference in contracts or memoranda of agreement as conditions for use of government office equipment and space.

Court unit officials may impose or maintain a more restrictive policy for personal use of government office equipment by their employees and other on-site personnel.

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

In using government office equipment for limited personal purposes, employees must, always, 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

- 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 electronic greeting cards, video, sound or other large file attachments, "push" technology on the internet, and other continuous data stream uses;

- Attempting to gain unauthorized access to other systems;

- Creating, copying, transmitting, or re-transmitting chain letters or other unauthorized mass mailings, regardless of subject matter;

- 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;

- Creating, downloading, viewing, storing, copying, transmitting, or re-transmitting sexually explicit or sexually oriented material;

- Creating, downloading, viewing, storing, copying, transmitting, or re-transmitting material related to gambling, illegal weapons, terrorist activities, and any other illegal or prohibited activities;

- 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;

- Using equipment for fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity;

- 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 public statements at variance with the judiciary mission or position;

- Using equipment in a manner that results in loss of productivity, interference with official duties, or greater than minimal additional expense to the government;

- Acquiring, using, reproducing, transmitting, or distributing without authorization any controlled information. Controlled information includes judiciary sensitive data (see: Guide, Vol. 15, § 310.10.10(e)), 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);

- Using judiciary-provided access to online investigative tools and databases containing personal information to gather information for non-work related purposes is prohibited, including attempting to research friends, neighbors, acquaintances, celebrities, other public figures, etc. Online investigative tools include LexisNexis and Westlaw public records or other databases that contain personal information (e.g., telephone, driver's license, auto registration and VIN numbers, home addresses, property ownership records, voting records).

## Management or Sanctions

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

# COMPUTER SECURITY

The following computer security standards apply:

## Password Management

Password management is a practical approach to protecting judiciary information and its associated IT infrastructure. A password is essentially a key that "opens the door" to information systems and the sensitive data stored within them. Secure password practices help prevent unauthorized users from accessing judiciary data.

The Court utilizes the mandatory password policy established by the Judiciary Enterprise Network Information Exchange (JENIE) and the National Active Directory (NAD) systems. Passwords must be a minimum of 10 characters and contain a minimum of 4 alphabetic characters and at least one numeric character. User Names and / or IDs are prohibited from using as portion of the password. A character may only be used three times within a password and the @ symbol is not allowed.

The initial login process for both the network and the national application systems will prompt the user every six months (180 days) to change the password.

Passwords should not be shared unless so directed by the Information Services Division. Normally, each user of the system will have a separate login account and unique password. Files may be shared by storing them in common subdirectories (I: or G:). Shared printers do not require login to be used.

## Anti-Virus Protections

All Court supplied IT assets (except for iDevices) are configured with anti-virus software with current malware definition. This is mandatory on all judiciary-owned and non-judiciary-owned IT assets (computers, laptops, servers, and mobile devices) that access judiciary networks, including virtual machines).

If an external storage device has been used in computers other than those in the court's system, it must be scanned for viruses before being used in a court computer. Users who are unfamiliar with scanning procedures must ask the Information Services Division for instructions. This policy includes all external storage devices from both internal or external sources.

Users must also be careful with files downloaded from the Internet. Currently Symantec Endpoint Protection is installed on all workstations and will automatically scan executable files that are downloaded. Beware of e- mail from people you don't know. Delete the message without reading it, because it could contain a virus.

## Personal Web Email Account Access

Access to personal web email accounts (e.g., Gmail, Yahoo, academic institutions) from within the DCN is restricted. Use of these accounts poses threats to the judiciary's IT infrastructure because web email messages and their attachments bypass the existing network anti-virus protections in place at the internet gateways and on the courts' email servers.

Sending sensitive judiciary information through personal web email accounts outside the judiciary network is also discouraged because the email accounts do not afford the user sufficient security or privacy.

## Employee Separation

When a user leaves the employment of the court, their manager is required to notify the Information Services Division. A separating employee notification is generated and all network accounts are terminated as of the date of separation. The IT staff coordinate with the separating employee or their supervisor to sign an IT Asset Transfer sheet. The IT Manger will then generate an Employee Separation memo as per Guide to Judiciary Policy, Volume 11: Internal Controls Section 670 Verification and Review (D) Periodic review of terminated or transferred individual system rights and email it to the appropriate HR department and CUE. After the user's files, have been reviewed for possible transfer or archiving, the account will be archived so that no one can log in with that user's name.

## Computer Security Awareness

As part of the new employee orientation, managers will ensure that new employees are fully aware of security procedures before they are granted access to the court's computer system. New employees will be required to complete the online Computer Security training, read the personal usage and computer security guideline, and sign the acknowledgement form.

Annually, all employees will be required to review these guidelines, sign the acknowledgment form and give to their Human Resource contact to be placed in their file.

If an employee experiences unusual computer symptoms while using the system (such as frequent crashes, strange messages on the screen, or sudden increases in file size) the Information Services Division must be notified immediately.

The Information Services Division will notify all system users whenever there is a security incident. Specific instructions will be given at that time for any enhanced security measures.

## Software

Word processing, spreadsheet, and other office applications are available on all court staff computers for performing official duties. They serve as tools for promoting efficiency and effectiveness in the court's functions. Personal use of this software is permissible outside of normal duty hours, but personal files should not be stored on the network.

No personal software may be installed or used on any court computer for three (3) primary reasons. First, all installed software must be licensed to the U.S. District Court, and using personal software on a court computer could violate copyright law. Second, using personal software increases the risk of infecting court computers with viruses. Third, the Information Services Division will not provide technical support for personal software. Employees are encouraged to recommend software to the IT manager or the clerk that may enhance the computer network.

**E-Mail**

Electronic mail is for official court business. Incidental use for short personal messages is permitted.

E-mail messages, which lend themselves to an informal writing style, should contain no words or phrases that would be considered offensive, harassing, or otherwise inappropriate. Creating, copying, transmitting, or re-transmitting chain letters or other unauthorized mass mailings, regardless of the subject is considered inappropriate.

Sending messages using someone else's login only with that person's permission should be "signed" with the actual sender's name. Personal E-mail accounts should not be accessed on a government computer.

**Network (Building Local Area Network and Wireless)**

To ensure the security and integrity of the Court's network resources, the Court's building local area network (BLAN) and wireless network are only to be connected to by Court supplied devices. Employees are prohibited from attaching personal laptops, wireless switches or any other networkable devices into the Court's BLAN. Employees are also prohibited from accessing the Court's wireless network using personal equipment such as laptops, smartphones, tablet pcs or any other network device.

**Internet**

Employees with a valid business-related need to use the Internet may be authorized by their supervisor to have access. While Internet usage is expected to be different for each employee having approved access, employees are permitted to use this resource only for official government business, except as otherwise provided in this policy. The Information Services Division may be instructed by the Judge/Unit Executive to monitor an individual's compliance with acceptable Internet use policies. Violation of applicable policies may result in discipline of the employee.

When accessing the Internet, employees must adhere to the same standards and code of conduct that govern all other aspects of judiciary employee activity. Because the Internet is an unsecured network, users should expect that communication and information transmission on the Internet are not private.

Prohibited activities on the Internet include but are not limited to the following:

1. Making unauthorized statements regarding court policies.

2. Transmitting confidential information.

3. Using subscription accounts or commercial services that are not related to official court business, for example: on-line purchasing and personal e-mail.

4. Posting an unauthorized or personal web page.

5. Engaging in personal chat room discussions or instant messaging (except for Court supplied instant messaging).

6. Viewing, sending or displaying obscene or sexually explicit material or any other material which may be inappropriate or reflect poorly on the judiciary.

7. Using government-provided Internet access to conduct personal business.

8. Using or distributing copyrighted material without the permission of the author or publisher.

9. Downloading files, except files from court approved sites (e.g., jnet, tsp, uscourts.gov).

10. Downloading programs (all programs should be downloaded and installed by the Information Services Department).

11. Accessing or using Social Media website unless special permission is granted by the user's manager as well as the IT Department and adhere to the Court's Social Media Policy.

## Electronic Device Policy

This electronic device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- laptop/notebooks/Surfaces
- tablets (iPad)
- mobile / cellular phones
- smartphones (iPhone)
- satellite phones
- home or Court supplied computer used to access the Court's resources
- any mobile device capable of storing Court's data and connecting to an unmanaged network.

## Laptop Policy

Laptops are available for checkout or assigned permanently to staff to complete work assignments while away from their normally assigned duty stations. After completion of a Check Out form, and a supervisor has approved the usage, a laptop will be provided (unless none is available). The laptop is to be returned on the date specified on the Check Out form unless permanently assigned.

The laptops are valued in excess of $2500.00. The employee takes full responsibility for repair or replacement of the laptop should the laptop be damaged or lost through negligence while the laptop is checked out to the employee.

## Take Home Policy for Court Supplied PC Equipment

Court staff will be allowed to maintain U.S. District Court personal computers at their residence to permit completion of work related tasks. The Unit Executive will approve each request. The computers will not be "supported" by the Information Services Division, therefore, care and maintenance will be provided by the unit staff trained in this function. Costs for Internet Access related to use of the personal computer in a private residence are the responsibility of the user.

The procedures for "take home" of government personal computers are derived from the Administrative Office's Volume 15: Information Technology, Section § 530 Use of Government-Owned IT Equipment Outside of Duty Station which specifically addresses this matter.

## Remote Access using personal/home computers

The Court provides remote access to the Court's resources for official court business only. To obtain access, the employee must have finished their "probationary period" and have their supervisor request a VPN/JPORT username and login from the IT Manager. Once a username and password have been established, the employee must undergo training from Information Services Division before using their account.

Users must provide the designated point of contact (e.g., service desk or personnel office) within their court unit, FPDO, or the AO, with a signed acknowledgment indicating that they understand the security risks involved and that they agree to maintain up-to-date versions of court-approved anti-virus software and use a firewall product with their personally or government-owned computer.

Security-related maintenance is performed by the user with instruction from the IT staff, or, when appropriate, by the IT staff directly.

Passwords and access codes must be carefully safeguarded. Family members and friends must never be given these passwords, nor should anyone other than the authorized user make use of remote access to judiciary networks. Passwords must not be saved or stored for automatic processing. Storing passwords on any computer is discouraged. However, using an encryption product (e.g., password vault software) to store passwords is acceptable.

## Court Supplied tablet computers (iPad)

The Court has standardized the Apple iPad as the primary tablet pc for use on the Court's network. Court staff who are assigned court supplied iPads are required to setup their iTunes account using a personal credit card and their court supplied email address. Court supplied applications are purchased through a main account that is linked to a government purchase card and then distributed through Apple iTune's "gifting" process. All other purchases are charged to the employee's personal credit card. Personal usage of the iPads fall under the permitted limited use of government office equipment for personal needs policy described earlier in the guidelines.

The iPads are valued in excess of $1500.00. The employee takes full responsibility for repair or replacement of the iPad should the iPad be damaged or lost through negligence while the iPad is checked out to the employee.

## Court Supplied iPhones

The Court has standardized the Apple iPhone as the primary smartphone for use on the Court's network. Personnel are to read and familiarize themselves with the operator's information related to the iPhone. Staff will be accountable for information contained in these documents. The iPhone must be kept charged and under control of the employee always.

iPhones have been provisioned with call and texting functionality and may be used for limited personal calls / texts as outlined below.

The cellular feature is activated on all iPhones and may be used for court business and limited personal calls. Personnel are strongly urged to use the "mobile to mobile" service to contact both court personnel and personal contacts if available. Since long distance and roaming are included, the court cellular phone should be used on travel to make calls to the office and authorized calls home. Reimbursement for using other methods to call home will not be authorized when an iPhone has been issued unless cellular services are unavailable.

Unlimited texting has been activated on all iPhones. Personal usage of texting fall under the permitted limited use of government office equipment for personal needs policy described earlier in the guidelines.

iPhones have been provisioned with data functionality and may be used as outlined below.

Data has been activated on all iPhones. These data plans include unlimited access for email and Internet on the smartphone only. Personal usage of iPhones fall under the permitted limited use of government office equipment for personal needs policy described earlier in the guidelines.

Data Tethering plans have been activated on some iPhones. These plans allow for the smartphone to provide Internet access for other devices such as laptops and iPads. These plans are limited to 4 GB of data transfer per month and incur an overage fee of $10 per 1 GB of data transferred. If data tethering has been activated on your device, usage is limited to Court supplied devices and work related tasks (remote access, internet based research, email). Personal usage of data tethering fall under the permitted limited use of government office equipment for

personal needs policy described earlier in the guidelines. Overage fees for non-Court related usage will be the responsibility of the employee.

Court staff who are assigned court supplied iPhones are required to setup their iTunes account using a personal credit card and their court supplied email address. Court supplied applications are purchased through a main account that is linked to a government purchase card and then distributed through Apple iTune's "gifting" process. All other purchases are charged to the employee's personal credit card. Personal usage of the iPhone falls under the permitted limited use of government office equipment for personal needs policy described earlier in the guidelines.

If the Court Unit Executive deems a substantial benefit to the Court (ie COOP Team members, Officers for field usage), court supplied iPhones can be designated as the primary mobile device for the employee and personal usage limitations will be waived.

## Court Supplied mobile/ cellular phones

Cell phones have been provisioned with call and texting functionality and may be used for limited personal calls / texts as outlined below.

The cellular feature is activated on most mobile devices and may be used for court business and limited personal calls. Personnel are strongly urged to use the "mobile to mobile" service to contact both court personnel and personal contacts if available. Since long distance and roaming are included, the court cellular phone should be used on travel to make calls to the office and authorized calls home. Reimbursement for using other methods to call home will not be authorized when a cell phone has been issued unless cellular services are unavailable.

Unlimited texting has been activated on all cell phones. Personal usage of texting fall under the permitted limited use of government office equipment for personal needs policy described earlier in the guidelines.

## Court Supplied Satellite Phones

Satellite phones have been assigned to certain key members of the Court's COOP team. Only the Chief Judge, Court Unit Executives, IT Manager, and Telephone Specialist are assigned active accounts. The remainder of the assigned satellites phones are not activated, but are configured to be activated on-demand.

## Monitor of devices with Cellular or Satellite Services

Monthly remote access and cellular/satellite voice/data logs will be reviewed by management. Each employee will be asked to account for any problems or discrepancies found in the logs.

The General Services Administration prohibits the use of electronic devices by a driver while operating a motor vehicle owned or leased by the federal government

## Damaged, Lost or Stolen Court Supplied Equipment

If court supplied equipment is damaged, lost or stolen the employee is to immediately report the problem to their supervisor and an IT Property Incident Report must be completed by the employee per our current ITAM Policy. In the case of theft, a police report is to be filed with the appropriate law enforcement authority and a copy turned in with the incident report. If it is determined by a Board of Survey that the equipment was damaged or lost due to neglect or misuse, replacement charges will be the responsibility of the employee.

# Personal Usage and Computer Security Acknowledgment Form

I have read the Personal Use of Government Equipment and Computer Security guidelines and acknowledge my responsibility to conform to the principles as a basis of computer use and security within the judiciary. I acknowledge that I will abide by all applicable policies.

Employee Name: _____

Title: _____

Signature: _____ Date: _____

# Remote Access Acknowledgement Form

(for VPN or JPORT users)

I have read the section on remote access in the Personal Use of Government Equipment and Computer Security guidelines and acknowledge the security risks involved and my responsibility to maintain up-to-date versions of court-approved anti-virus software and use a firewall product on my personal or government-owned computer.

Employee Name: _____

Title: _____

Signature: _____ Date: _____