



---

**INTERNAL REVENUE SERVICE (IRS) POLICY ON LIMITED PERSONAL USE OF  
GOVERNMENT INFORMATION TECHNOLOGY EQUIPMENT/RESOURCES**

**1. PURPOSE**

This policy defines acceptable personal use of government information technology equipment/resources by IRS employees. This policy supplements IRS Policy on Electronic Communications of 10/21/97 (transmitted by memorandum on 6/6/00).

**2. BACKGROUND**

The Executive Branch of the Federal Government serves the American people through hundreds of thousands of employees located in offices across the nation. Increasingly, the Government is called on to deliver more and better services to a growing population that continues to expect ever-increasing improvements in service delivery. Many of these improvements come about through the use of modern information technology such as computers and the Internet. This expanding use of technology in the workplace offers new opportunities to provide a supportive environment for employees, always balancing the overriding imperative that the American taxpayers receive the maximum benefit for their tax dollars. Public confidence in the productiveness of the IRS is increased when the public is confident that the Service is well managed and assets are appropriately used. The need to maintain public confidence must always be considered in developing any Service policy.

In light of the expansion of information technology equipment/resources to an ever expanding group of Service employees, the recent issuance of Treasury Directive 87-04 "Personal Use of Government Office Equipment Including Information Technology", and the desire of the Service to enhance the quality of the workplace, a policy allowing limited personal use of information technology equipment and resources has been developed.

**3. SCOPE**

The policy applies to all IRS employees, including detailees, temporary employees, and interns performing work for the IRS (hereafter called employees), whether the employee is working in a Government-designated office, traveling, or working from home on behalf of the Service. This benefit/privilege is not extended to contractors.

**4. POLICY**

It is the policy of the IRS to:

- a. allow employees the privilege to use government information technology equipment/resources for other than official Government business, when such use involves minimal additional expense to the government, does not overburden any of the Service's information resources and when access to these technology equipment/ resources is already authorized for official government business. IRS is not required to provide access to these resources if they are not already provided for an approved business need.



- 
- b. permit such limited personal use to employees during non-work time for reasonable duration and frequency of use.
  - c. grant use that does not adversely affect the performance of official duties, interfere with the mission or operations of the IRS.
  - d. authorize use that does not violate the Office of Government Ethics (OGE) Standards of Ethical Conduct for Employees of the Executive Branch found at 5 Code of Federal Regulations (CFR) Part 2635, the Supplemental Standards of Ethical Conduct for Employees of the Treasury Department found at 5 CFR Part 3101 and the Department of the Treasury Employee Rules of Conduct found at 31 CFR Part 0.

The policy establishes new privileges and additional responsibilities for employees. The personal use of government information technology equipment/resources requires responsible judgement, supervisory discretion and compliance with applicable laws and regulations. See Appendix A, for specific guidance applicable to this policy. Employees must be aware of information technology security issues which are addressed in the Internal Revenue Manual (IRM) 25.10.1, Information Technology (IT) Security Policy and Guidance, as well as any other IRS privacy concerns related to the safeguarding of sensitive information.

## 5. DEFINITIONS

- a. *Employee non-work time* means times when the employee is not otherwise expected to be addressing official business. Employees may, for example, use government information technology equipment/resources during their own off-duty hours such as before or after a workday, lunch periods, authorized breaks, or weekends or holidays. For employees using government information technology equipment/resources in a government facility, no expanded access to the building will be provided beyond when the building is normally open for access.
- b. *Government information technology equipment/resources* for the purpose of this policy is limited to personal computers and related peripheral equipment and software, personal digital assistants (such as Palm Pilots), facsimile machines, photocopiers and connectivity and access to Internet services and e-mail. This policy does not cover access to the IRS Intranet.
- c. *Minimal additional expense* means that employee's limited personal use of government information technology equipment/resources is limited to those situations where the government is already providing equipment or resources and the employee's use of such equipment or services will not result in any additional expense to the government or the use will result in only normal wear and tear, or the use of small amounts of electricity, paper etc. Examples of minimal additional expenses include using a computer printer to print out a few pages of material, infrequently sending personal e-mail messages, or limited use of the Internet for personal reasons.
- d. *Limited personal use by employees during personal time is considered an "authorized use"* of government property as the term is used in the Standards of Conduct for Employees of the Executive Branch (5 CFR § 2635.101 (b) (9) and § 2635.704 (a)). Employees are specifically prohibited from the pursuit of private commercial business activities or profit-making ventures using the government's information technology equipment/resources. The ban also includes employees' using the government's information technology equipment/resources to assist

---

relatives, friends, or other persons in such activities (e.g., employees may not operate or participate in the operation of a business with the use of the Service's computers and Internet resources).

- e. *Privilege*, in the context of this policy, means that the Service is extending the opportunity to its employees to use government information technology equipment/resources for limited personal use in an effort to create a more supportive work environment. However, this policy does not create the right to use government information technology equipment/resources for other than official Government business. Nor does the privilege extend to modifying the equipment used, including loading personal software, copying existing software, or making configuration changes.

## 6. RESPONSIBILITIES

- a. The Deputy Commissioner of Modernization/Chief Information Officer has Servicewide responsibilities to manage information technology (IT) including IT security and will disseminate additional policy appropriate to this subject as necessary.
- b. Heads of Offices are responsible for ensuring that this policy is disseminated to all employees.
- c. Managers should ensure that employees are informed of appropriate uses of government information technology equipment/resources as a part of their introductory training, orientation or the initial implementation of this policy (See Appendix A - Specific Guidance). Managers are also responsible for ensuring that information technology/resources are being used appropriately and for taking corrective action, as needed.
- d. Employees are accountable to follow rules and regulations and to be responsible for their own personal and professional conduct. The OGE Standards of Ethical Conduct states, "Employees shall put forth honest effort in the performance of their duties" (5 CFR § 2635.101 (b)(5)). In addition, the Office of Personnel Management (OPM) Employee Responsibilities and Conduct states, "An employee shall not engage in criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, or other conduct prejudicial to the Government" (5 CFR § 735.203).

## 7. AUTHORITY

- a. 5 CFR Part 2635, Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch
- b. 5 CFR Part 3101, Supplemental Standards of Ethical Conduct for Employees of the Department of the Treasury
- c. 31 CFR Part 0, Department of the Treasury Employee Rules of Conduct
- d. 5 CFR Part 735, Office of Personnel Management, Employee Responsibilities and Conduct

## 8. REFERENCES

- a. 5 CFR § 2635.101 (b)(5) and (9), Basic Obligation of Public Service



- 
- b. 5 CFR § 2635.702 (b), Appearance of Governmental Sanction
  - c. 5 CFR § 2635.704 (a) and (b)(1), Use of Government Property
  - d. 5 CFR § 2635.705, Use of Official Time
  - e. 5 CFR § 735.203, Conduct Prejudicial to the Government
  - f. 31 CFR § 0.213, General Conduct
  - g. (FPMR) 41 CFR § 101-35.201
  - h. Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Resources"
  - i. TD P 71-10, Department of the Treasury Security Manual  
<http://Intranet.cio.treas.gov/sites/cio/mag3/securityfs.htm>
  - j. j. TD P 81-01, Department of the Treasury Information Technology (IT) Manual
  - k. TD 87-04, Personal Use of Government Office Equipment Including Information Technology (May 17, 2001)
  - l. 1. IRM 6.751.12, Guide to Penalty Determinations, Exhibit 6

Attachment

---

**Appendix A****Specific Guidance****1. Specific Provisions on the Limited Personal Use of Government Information Technology Equipment/Resources**

Under this policy, employees are authorized limited personal use of government information technology equipment/resources. IRS is not required to provide access to these resources if they are not already provided for an approved business need. For the purpose of this policy, government information technology equipment/resources is limited to personal computers and related peripheral equipment and software, personal digital assistants (such as Palm Pilots), photocopiers, facsimile machines, and connectivity and access to Internet services and e-mail. This policy does not cover access to the IRS Intranet.

This personal use must not result in loss of employee productivity or interference with official duties. Moreover, such use should incur only minimal additional expense to the Government in areas such as:

- a. communications infrastructure costs; e.g., Internet access, etc.;
- b. use of consumables in limited amounts; e.g., paper, ink, toners, etc.;
- c. general wear-and-tear on equipment;
- d. minimal data storage on storage devices; and
- e. minimal transmission impacts with moderate e-mail message sizes with small attachments.

**2. Inappropriate Personal Uses**

Employees are expected to conduct themselves professionally in the workplace and to refrain from using government information technology equipment/resources for activities that are inappropriate based on established standards of conduct. In addition, some restrictions are necessary to avoid practices that have the potential of degrading the overall performance of IRS systems. Misuse or inappropriate personal use of government information technology equipment/resources includes but is not limited to:

- a. the creation, copying, transmission, or retransmission of greeting cards, video, sound or other large file attachments that can degrade the performance of the entire network or the use of e-mail practices that involve ongoing message receipt and transmission (referred to as instant messaging/messenger). "Push" technology on the Internet (e.g. subscribing to any unofficial service such as EntryPoint or LaunchPad that gathers information and sends it out automatically to subscribers) and continuous data streams (such as streaming stock quotes) would also degrade the performance of the entire network and would be an inappropriate use;
- b. access to hacker sites (sites open the Service to unacceptable security risk);
- c. access to pornography sites;



- 
- d. using Government systems as a staging ground or platform to gain unauthorized access to other systems;
  - e. the creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter;
  - f. using government office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation;
  - g. the creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials;
  - h. the creation, download, viewing, storage, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited;
  - i. downloading, copying, and/or playing of computer video games;
  - j. use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services);
  - k. engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity;
  - l. use for posting agency information to external news groups, bulletin boards or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate agency approval has been obtained or the use is not at odds with the agency's mission or positions;
  - m. any use that could generate more than minimal additional expense to the government (e.g., subscribing to unofficial LISTSERV or other services which create a high-volume of e-mail traffic);
  - n. the unauthorized acquisition, use, reproduction, transmission, or distributions of any controlled information including computer software and data, that includes privacy information, copyrighted, trade marked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data;
  - o. any use that reduces productivity or interferes with the performance of official duties;
  - p. any access to personal e-mail accounts through the Internet (e.g. accessing personal AOL accounts through IRS Internet firewall);
  - q. any access to Internet that does not go through an IRS approved Internet gateway (i.e. firewall). Accessing the Internet from non-office locations using a government owned computer must



---

always be done via the IRS approved Internet gateway; using any other connection (such as a private AOL account) is prohibited.

- r. any use of a photocopier or facsimile machine that involves more than a few pages of material (e.g. copying a book, making numerous copies of a resume, or sending/receiving a lengthy document via facsimile machines).
- s. any use of photocopiers or facsimile machines that conflicts with the need to use the equipment for official business requirements.

### **3. Proper Representation**

It is the responsibility of employees to ensure that they are not giving the false impression that they are acting in an official capacity when they are using government information technology equipment/resources for non-government purposes. If there is expectation that such a personal use could be interpreted to represent an agency, then an adequate disclaimer must be used. One acceptable disclaimer is -"*The content of this message is mine personally and does not reflect the position of the U.S. Government, the Department of the Treasury or the Internal Revenue Service.*"

The OGE Standards of Ethical Conduct states - "...an employee shall not use or permit the use of his Government position or title or any authority associated with his public office in a manner that could reasonably be construed to imply that his agency or the Government sanctions or endorses his personal activities" (5 CFR § 2635.702 (b)). In addition, 5 CFR § 2635.704 concerning the use of Government property, CFR § 2635.705 use of official time and 31 CFR § 0.213 concerning general conduct should be reviewed.

### **4. Access Management**

The privilege accorded by this policy is limited to the availability of government information technology equipment or resources; it may not conflict with the need to use the equipment for the performance of official duties. Therefore, restrictions may be imposed to address any capacity, security or other operational issues that might arise. IRS management retains the right to monitor both the content and the level of access of employees' personal use of government technology resources and equipment. This monitoring does not include use of the IRS Intranet.



**5. Privacy Expectations**

Executive Branch employees do not have a right, nor should they have an expectation, of privacy while using any government information technology equipment/resources at any time, including accessing the Internet or using e-mail. To the extent that employees wish that their private activities remain private, they should avoid using government information technology equipment/resources such as their computer, the Internet or e-mail. By using government information technology equipment/resources, executive branch employees give their consent to disclosing the contents of any files or information maintained using government equipment/resources. In addition to access by the Service, data maintained on Government office equipment may be subject to discovery and Freedom of Information Act requests.

By using government information technology equipment/resources, consent to monitoring and recording is implied with or without cause, including (but not limited to) accessing the Internet or using e-mail. Any use of government information technology equipment/resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

Privacy expectations related to the IRS Intranet are not covered by this policy.

**6. Sanctions for Misuse**

Unauthorized or improper use may result in loss of use or limitations on the use of the information technology equipment/resources, disciplinary or adverse actions, termination, criminal penalties and/or the employee's being held financially liable for the cost of improper use.