Department of the Treasury	Internal Revenue Service	Office of Chief Counsel	**Notice**

CC-2011-016

July 22, 2011

Subject:	Chief Counsel Policy on Limited Personal Use of Government Technology Equipment / Resources	**Cancel Date**:	Upon incorporation into the CCDM

I. BACKGROUND

This CCDM notice is being issued to update the Office of Chief Counsel's existing limited personal use policy. The policy is being updated to reflect current technologies, current practices on blocking accesses to sites, and to clarify several points.

The most important changes are: a clear rule that employees should not download computer programs, including executable code, and a clarification of how limited personal use interacts with approved "pro bono" legal activities of Counsel attorneys.

II. GENERAL RULE

Under the terms and conditions defined in this Notice, Counsel employees will be allowed limited personal use of government computers and systems. Employees should note that the privilege of using Government office equipment (including information technology) for non-governmental purposes comes with restrictions as specified in this policy. Employees must be aware of information technology security issues which are addressed in the Internal Revenue Manual (IRM) 10.8.1 as well as any other privacy concerns related to the safeguarding of sensitive information.

It is the policy of the IRS Chief Counsel 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 information resources, and when access to these technology equipment / resources is already authorized for official government business. The Office of Chief Counsel 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 during non-work time for reasonable duration and frequency of use.

Distribute to:	X All Personnel		
	X Electronic Reading Room		
Filename:	CC-2011-016	File copy in:	CC:FM:PM

C. Grant use that does not adversely affect the performance of official duties, interfere with the mission or operations of the IRS or the Office of Chief Counsel.

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.

III. WHAT USES ARE PROHIBITED?

A. 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 Counsel and IRS systems.

B. Prohibited uses of government technology, equipment and resources by employees (even on non-work time) include, but are not limited to:

1. Downloading, copying, or installing of unauthorized application (e.g., executable code) or any program not explicitly approved or permitted by the organization(s) with responsibility for managing data programs, such as:

   a) Screen savers,

   b) Software products,

   c) “Push” technology applications (subscriber services) from the Internet (e.g., weather or news alert feeds, stock quote updates) that gather information and send it out automatically to a subscriber,

   d) Test or demo software, and

   e) Computer games.

2. Personal communication on blogs and social networking sites such as Facebook, MySpace, Yahoo! 360°, Twitter, etc.;

3. Viewing or accessing the following types of web sites:

   a) Pornographic, sexually explicit, or sexually oriented materials (including creation, download, viewing, storage, copying of such materials); or

   b) Personal services web sites, such as Personals & Dating and Craigslist.

4. Access to hacker sites (regardless of the security risks or lack thereof);

5. Using Government systems as a staging ground or platform to gain unauthorized access to other systems;

6. On-line games;

7. 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;

8. 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;

9. 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, or sale of goods or services). This 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 government computers and internet resources);

   Important exception for Counsel attorneys:
   Counsel attorneys who are engaged in officially-approved outside “pro bono” legal activities (not on behalf or relatives or friends) will be allowed limited personal use of government computers (and other IT equipment / technology) during non-work time for these approved “pro bono” purposes.

10. Engaging in any outside fund-raising activity (including political fund-raising), endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity;

11. 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;

12. 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);

13. Unauthorized acquisition, use, reproduction, transmission, or distribution 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 including copyrighted materials, such as music, videos, and pictures;

14. Any use that reduces productivity or interferes with the performance of official duties;

15. Any access to personal e-mail accounts through the Internet (e.g. accessing personal AOL accounts, hotmail accounts or company accounts through Office of Chief Counsel internet firewall);

16. Any access to internet that does not go through an Office of Chief Counsel approved internet gateway / firewall. Accessing the internet from nonoffice locations using a government owned computer must always be done via the Office of Chief Counsel approved internet gateway — using any other connection (such as a private AOL account) is prohibited.

17. Use of peer-to-peer (P2P) file sharing software and networks. P2P refers to any software or system allowing individual users of the Internet, intranet or extranet to connect and share files or resources. Engaging in P2P practices creates a substantial computer security risk in that P2P may facilitate the spread of computer viruses. Specific examples of P2P file sharing include applications such as Morpheus, Napster, Grokster, Kazaa, and Gnutella, as well as decentralized applications such as SETI@Home.

18. Inappropriate use of IRS e-mail account(s), such as:

    a) Transmitting files larger than 5 megabytes,

    b) Any correspondence for personal gain (Avon, private commercial business, selling of personal goods or services, etc),

    c) Solicitation of employees, such as Girl Scout or Boy Scout fund raisers, and

    d) Chain letters or other unauthorized mass mailings regardless of the subject matter;

19. Creation, copying, transmission, download, storage, or retransmission of prohibited materials;

20. 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); and

21. Any use of photocopiers or facsimile machines that conflict with the need to use the equipment for official business requirements.

IV. CONSEQUENCE FOR MISUSE

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. Counsel management retains the right to monitor both the content and the level of access of employees' personal use of government technology resources and equipment. The Office of Chief Counsel has systems in place which monitor internet use at individual workstations and systems that block access to some inappropriate sites.

Employees who access inappropriate sites (including, but not limited to, sexually related sites) or otherwise violate the rules regarding limited personal use will be subject to disciplinary or adverse actions, up to and including removal.

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

V. SCOPE, PROPER REPRESENTATION, AND DEFINITIONS

A. SCOPE

The policy applies to all Chief Counsel Employees, including detailees, temporary employees and interns performing work for the Office of Chief Counsel (hereafter called employees), whether the employee is working in a Government-designated office, traveling, or working from home (typically referred to as “flexiplace”) on behalf of the Office of Chief Counsel. This benefit/privilege is not extended to contractors.

B. 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 IRS Office of Chief Counsel."

C. DEFINITIONS

1. 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, 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.

2. 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 Blackberries, cell phones, Palm Pilots), facsimile machines, voice mail, photocopiers and connectivity and access to internet services and e-mail. This policy does not cover access to the Office of Chief Counsel/IRS intranet.

3. 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 beyond the following:

    a) Communications infrastructure costs (e.g., internet access);

    b) Use of consumables in limited amounts; e.g., paper, ink, toners;

c) Normal wear-and-tear on equipment;

d) Minimal data storage on storage devices; and

e) Minimal transmission impacts with moderate e-mail message sizes that with attachments are no larger than 5 megabytes.

4. 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.

5. Limited personal use activity by employees that is conducted during personal time in the course of the business day 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)).

6. Privilege, in the context of this policy, means that Counsel 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.

VI. PRIVACY ISSUES

Employees do not have a right to, and should not expect, privacy while using government information technology, equipment and/or 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 Office of Chief Counsel or the IRS, 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.

/s/
Dennis M. Ferrara
Associate Chief Counsel
(Finance & Management)