MS 547 Use of Government Technology Services and Equipment

Effective Date: June 30, 2014
Responsible Office: Office of the Chief Information Officer
Supersedes: 1/7/13; 11/22/11

Issuance Memo 06/30/14
Issuance Memo 01/07/13
Issuance Memo 11/22/11

Table of Contents

1.0 Purpose

This Manual Section establishes Peace Corps policy for the use of government technology services and equipment. This policy applies to Peace Corps employees, including personal services contractors, and Peace Corps contractors and others with access to U.S. Government technology, services and equipment.

2.0 Authority

E.O 12674, OMB A-130, the Office of Management and Budget Memorandum M-04-26, and the Clinger-Cohen Act.

3.0 Definition

Government technology services and equipment include Peace Corps–purchased and/or –owned computer services, equipment, or interconnected system or subsystems that are used in the automated acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Peace Corps. Equipment and services can include, but are not limited to, computing devices and

related peripheral equipment (e.g., laptops, tablets, desktop computers, local and networked printers, copiers, faxes, and multi-function devices (MFDs)), online and offline reference resources, mobile and land based telecommunications devices (e.g., voice over internet protocol (VoIP) phones, smart phones, air cards, video cameras), computer software or firmware, Internet connectivity, and support services.

4.0 Policy

4.1 Official and Authorized Activity

The Peace Corps communication network is for intra-agency controlled unclassified information and Peace Corps Sensitive Information (see procedures issued under MS 542 *Information Technology Policy*). All users of the Internet and Peace Corps Intranet through Peace Corps services must comply with the security requirements set forth in the Rules of Behavior for General Users (see procedures issued under MS 542 *Information Technology Policy*). Standards regarding the content and usage of e-mail transmitted on Peace Corps communication networks are also contained in the Rules of Behavior for General Users and include the following:

(a) Employees must use common sense and good judgment when using technology services and equipment and must understand and avoid the unnecessary accumulation of usage fees that are not fixed or flat rate.

(b) Employees must avoid international roaming charges for mobile phones when other telecommunications devices and services are available. Alternatives and other practices are documented in guidelines (e.g., Mobile Devices Practices) issued by the Office of the Chief Information Officer (OCIO). Employees are responsible for understanding and applying these practices when using equipment assigned to them or when using loaner equipment acquired from the OCIO.

(c) Except as specifically provided in laws or regulations, employees who use government technology services and equipment are not covered by the privacy protections applicable to the use of personal technology services and equipment. The Peace Corps, through the Chief Information Officer and other agency officials, such as system managers and supervisors, employs monitoring tools to detect inappropriate personal use of government technology services and equipment. They may, as needed, access any employees' electronic communications or files.

(d) Each employee is responsible for his/her own actions. Supervisors are responsible for oversight and management of employees' activities and determining which uses of government technology services and equipment are inappropriate.

(e) The conduct of official government business always takes precedence over any limited personal use.

4.2 Limited Personal Use

Use of government technology services and equipment, including access to the Internet, is for official use by authorized personnel. Limited personal use (using government equipment for purposes other than accomplishing official or otherwise authorized activity) is allowed as provided in this Manual Section. However, personal use is a privilege and not a right, and may be revoked or limited at any time at the discretion of an employee's supervisor or the Chief Information Officer. Personal use is subject to the following rules:

(a) Employee personal use of government equipment must not adversely affect the employee's performance; must be of reasonable duration and frequency; and involve activities that cannot reasonably be done at another time.

(b) Personal use is limited to situations where the government is already providing equipment or services and the employee's use of the equipment or services will not result in any additional or only minimal expense to the government, or the use results in only normal wear and tear or in the use of small amounts of such items as electricity, ink, toner, or paper. It is the employee's responsibility to be aware whether any additional cost is involved.

(c) Examples of limited personal uses that involve minimal additional expense include: making a few photocopies; printing a few pages from a computer printer; making domestic phone calls, sending text messages, or email using a mobile device that is provided at a flat-rate fee to the agency such that fees are not dependent on usage (e.g., roaming charges); infrequently sending personal email messages; or making limited use of the Internet for personal reasons.

4.3 Inappropriate Personal Use

Inappropriate personal use of government technology services and equipment, regardless of whether the use occurs on or off government premises or whether the use is during or outside normal work hours, includes:

(a) Any personal use that could cause congestion, delay, or disruption of performance to any government network, system, or equipment (e.g., transmission or storage of electronic files such as greeting cards, video, sound, large file attachments, "push" technology on the Internet, and continuous data streams such as websites that stream movie, live-video, sports events, or music).

(b) Use of any government system or service as a staging ground or platform to gain unauthorized access to other systems.

(c) The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.

(d) Use 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.

(e) The creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials.

(f) The creation, downloading, viewing, storage, copying, or transmission of materials related to gambling, illegal weapons, terrorist activities, or any other illegal or prohibited activities.

(g) 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).

(h) Use to engage in any outside fund-raising activity, to endorse any product or service, to participate in any lobbying activity, or to engage in any prohibited partisan political activity.

(i) Use for posting Peace Corps information to external newsgroups, bulletin boards, or other public forum without authority. This includes any use at odds with the Peace Corps mission or positions, or that could create the perception that the communication was made in one's official capacity as a federal government employee.

(j) The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data, that includes privacy information; proprietary data; export controlled software or data; or material that is copyrighted, trademarked, or to which other intellectual property rights attach (beyond fair use).

The Chief Information Officer (CIO) may restrict access to any website if (1) access to that website has a material negative impact on Agency network security or the availability of Peace Corps Internet connectivity and (2) there is no legitimate business need for access to that website. The CIO will provide advance notice of the intention to restrict access to a website so that those staff having a legitimate business need for access to that website can make their need known to the CIO. Requests not to restrict a website should be documented and directed to the CIO. The CIO will publish on the agency Intranet a list of all websites to which access is restricted.

4.4 Disclaimers Regarding Personal Use

It is the responsibility of employees to ensure that they do not give the false impression that they are acting in an official capacity when they are using government technology services or equipment for limited personal use. When using Peace Corps technology services and equipment, employees must use a disclaimer for any personal communication that could reasonably be interpreted as an official Peace Corps statement or action. One acceptable disclaimer is: "*The contents of this message are mine personally and do not reflect any position of the U.S. government or the Peace Corps."*

By using government technology services or equipment, employees acknowledge that, except as otherwise protected by laws or regulations, the contents of any files or information maintained or passed through government technology services or equipment may be accessible to the Peace Corps and their use of such technology may be monitored and recorded, with or without cause, including but not limited to their access to the internet and use of electronic communications.

5.0 Sanctions for Inappropriate Personal Use

An employee's unauthorized or inappropriate personal use of government technology services and equipment could result in sanctions against the employee, including loss of use or limitations on use of services and equipment, disciplinary or adverse administrative actions, criminal penalties, and/or financial liability for the cost of any inappropriate personal use.

6.0 Effective Date

The effective date is the date of issuance.