MS 543 USE OF IT SYSTEMS BY VOLUNTEERS, TRAINEES, AND RETURNED PEACE CORPS VOLUNTEERS

Date: April 3, 2008
Responsible Office: OCIO
New Manual Section Supersedes: June 22, 2006; IPS 3-02, Guidelines for Volunteer Use of IT Systems; IPS 4-02, Use of PC IT Systems by RPCVs; and Guidance Regarding Volunteer Access to, and Use of, Computer Equipment and Information Technology (Baquet Memo), February 15, 2001.

TABLE OF CONTENTS

ATTACHMENTS

Attachment A Volunteer Computer Guidelines Signature Form
Attachment B RPCV Computer Usage Form
Attachment C Mandatory Guidelines for RPCV Use of Peace Corp-Provided IT Equipment

SUBSECTION A: PURPOSE AND GENERAL POLICIES

1.0 PURPOSE

The purpose of this manual section is to set out the mandatory guidelines on the use of Peace Corps and non-Peace Corps IT equipment by Volunteers and Trainees (V/Ts), and the use of Peace Corps IT equipment by Returned Peace Corps Volunteers (RPCVs). Violations of the policies or guidelines in this manual section are grounds for disciplinary action up to and including administrative separation (V/Ts) or revocation of the privilege of using the Peace Corps IT equipment (RPCVs).

2.0 POLICIES

2.1 Peace Corps-owned computers are made available overseas to V/Ts. V/Ts are required to comply with the mandatory guidelines on the use of such computers as set out in this manual section. "V/T computers" are shared by many V/Ts, and are set up in a standard way to ensure that the data are secure and that the computers are stable. Volunteers shall not attempt to change the computer setup in any way, including installing applications and/or changing settings. Any changes to the setup in any way may cause instability, security vulnerabilities, licensing problems, incompatibilities, and other problems that make the computer less productive for other Volunteers.

If any such changes are made, Peace Corps IT staff will need to reformat and reconfigure the affected computer in order to restore it to the standard setup. If such action is required, Volunteer data will be lost on that particular computer and the V/T's ability to access the computers and/or the Internet may be lost.

2.2 Peace Corps has software and systems in place that can monitor and record all Internet usage. The Agency reserves the right to inspect any and all files and devices stored in shared and non-shared areas of the Agency's network in order to ensure compliance with Peace Corps policies. There is no right to privacy on Peace Corps computers or networks.

2.3 A V/T may participate in Peace Corps systems, such as online collaborative tools, only upon Agency authorization.

2.4 V/Ts must review the mandatory guidelines set out below, and sign the form in Attachment A verifying that they will abide by the guidelines.

3.0 MANDATORY GUIDELINES

V/Ts must comply with the following basic requirements:

(a) Under NO circumstances are V/Ts allowed to use staff computers or computers of Volunteer Leaders/Coordinators. V/Ts may use the Volunteer Workstations;

(b) V/Ts shall read and follow the Peace Corps Inappropriate Internet Usage Guidelines in Section 4.0 below;

(c) V/Ts shall take reasonable precautions to protect IDs and passwords issued to them by Peace Corps for use on Peace Corps systems and shall not share them with any person.

(d) V/Ts shall not install software on the Volunteer workstations, including games, instant messaging, internet chat programs, or utilities;

(e) When finished using the computer, V/Ts shall log out to prevent unauthorized use and to protect documents;

(f) V/Ts shall use a password protected screen saver when the V/T is not at his or her station;

(g) V/Ts may not boot a computer from any source other than the standard hard drive, such as from a CD, USB drive, or other memory device; and

(h) V/Ts may not leave any hardware or software on computers when they leave the machine, including cameras, loggers, or other similar devices.

4.0 INAPPROPRIATE INTERNET USAGE AND SYSTEM USAGE

V/Ts shall not engage in any inappropriate Internet usage. Inappropriate Internet usage includes:

(a) Any personal use that could cause congestion, delay, or disruption of service to any government system or equipment. Examples of uses include, but are not limited to: greeting cards, large file attachments (including video and sound), "push" technology on the Internet such as Really Simple Syndication services, and continuous data streaming such as RealPlayer, Quicktime, Windows Media, or Voice Over IP (telephone) services. (Business use of these technologies must be approved by the OCIO);

(b) Use of any government system for any "hacking" or "cracking," including as a staging ground or platform to gain unauthorized access to other systems;

(c) Knowingly creating, copying, transmitting, or retransmitting chain letters or other unauthorized mass mailings, regardless of the subject matter;

(d) Use of the Internet for activities that are illegal, inappropriate, or offensive to peers 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 for non-business purposes;

(f) The creation, downloading, viewing, storage, copying, or transmission of materials for participation in gambling, illegal weapons, terrorist activities, or any other illegal or prohibited activities;

(g) The deliberate propagation of any virus, worm, Trojan horse, or other form of malicious code;

(h) The re-use of your Peace Corps network user ID or passwords for access to non-Peace Corps computer systems or any Internet sites, such as Hotmail, AOL, etc.;

(i) The downloading of any software, for example, to staff or Volunteer computers, unless prior approval has been obtained through existing Peace Corps procedures. This includes shareware and freeware such as AOL Instant Messenger;

(j) The attempt to disable, defeat, or circumvent any Peace Corps security resource or service;

(k) The transmission of files containing sensitive data that are transferred in any way across the Internet without appropriate encryption;

(l) Use of the Internet for profit or monetary gain, such as operating a business;

(m) Disclosure of personal or proprietary information of the Peace Corps; and

(n) Publication of copyrighted material without the express written permission of the copyright holder.

SUBSECTION B: POLICIES APPLICABLE TO BOTH PEACE CORPS AND NON-PEACE CORPS-OWNED EQUIPMENT AND SERVICES

5.0 APPROPRIATE USE OF INFORMATION TECHNOLOGY SYSTEMS AND SERVICES

5.1 Country Directors should advise V/Ts to use discretion and judgment when using Peace Corps or non-Peace Corps-owned computer equipment. This is of particular importance when communicating via e-mail or the Internet, which have the potential for mass distribution. V/Ts are free to discuss their role in the Peace Corps with any individual or group, but they should recognize that ill-considered statements could be used to embarrass themselves, the host country in which they serve, the Peace Corps, or the United States. Material that might be viewed as disparaging to the host country or as politically sensitive by the host government could create significant problems for the Peace Corps program in that country. The care one takes in private communication should be no less than the care taken in public utterances; messages to friends and family or the contents of web pages may be passed to the press or others and become a public issue.

5.2 V/Ts should be made aware of Peace Corps policies regarding publication of materials, political expression, and other related issues, which are discussed in the Volunteer Handbook and MS 204, Volunteer Conduct, when they use IT systems and services, such as e-mail, blogs, text messaging, and posting material to the Internet.

5.3 V/Ts should also be made aware of the potential for violation of U.S. privacy, host country, or other applicable laws if they include in any electronic communication (e.g., e-mail, blogs, text messages, or a web page) detailed personal information about individuals, such as full names or addresses, without the specific prior permission of those individuals. In addition, V/Ts could potentially violate such laws if they transmit information that could be defamatory in nature regarding another individual. Similar restrictions may apply to the unauthorized transmission or posting of a person's photograph or likeness. Social security numbers should never be posted on a Web site or transmitted via e-mail, under any circumstances.

5.4 Volunteer Contributions to Peace Corps' Official Web Sites

The Office of Communications, which oversees the Peace Corps' official external web site (http://www.peacecorps.gov), welcomes the submission of essays, stories, and photographs from Volunteers that will assist in highlighting Peace Corps activities to prospective applicants and the general public. All submissions should be reviewed by the Country Director and forwarded to the Office of Communications for consideration. Country Directors are encouraged to broadly distribute this guidance, and any applicable country-specific guidelines, to staff and Volunteers. Such information should be posted in appropriate areas such as in-country resource centers or other facilities with Peace Corps-owned computer equipment. Country Directors should also ensure that this information is reflected in Volunteer Assignment Descriptions (VADs), Welcome Books, and other recruitment materials.

SUBSECTION C: POLICIES APPLICABLE TO USE OF NON-PEACE CORPS IT EQUIPMENT AND SERVICES

6.0 USE OF EQUIPMENT OF OTHER ENTITIES

The extent to which V/Ts have access to computer equipment owned by other entities, such as a sponsoring agency, local non-governmental agency, or private donor, may vary from post to post. V/Ts who use such equipment should follow applicable computer use policies and be aware that the Peace Corps will not be responsible for the maintenance or replacement of the equipment. In addition, V/Ts are encouraged to purchase personal property insurance to cover the maintenance and replacement of computer equipment that they bring overseas or purchase in-country.

7.0 WEB SITES

Volunteers who create their own Web sites, or post information to Web sites that have been created and maintained by others, should be reminded that, unless password protected, any information posted on the Internet can be accessed by the general public, even if that is not intended. Because search engines regularly index most sites on the Internet, it is possible that members of the public could locate a Volunteer Web site by searching for information about the Peace Corps or a certain country. This is possible even if the Volunteer does not actively promote his/her Web site. Given these realities, Volunteers are responsible for ensuring that their IT use is consistent with the following guidelines:

7.1 Notification

Volunteers who create their own Web sites or post material to Web sites created by others are responsible for discussing the content in advance with the Country Director to ensure that the material is suitable and complies with this general guidance as well as any country-specific guidance.

7.2 Disclaimer

Any web site maintained by a Volunteer during his or her Peace Corps service must reflect the fact that it is not an official publication of the Peace Corps or the U.S. Government. The site, therefore, must be labeled clearly and prominently with an appropriate disclaimer such as: "The contents of this Web site are mine personally and do not reflect any position of the U.S. Government or the Peace Corps."

7.3 Use of the Peace Corps Logo

Because use of the Peace Corps logo is reserved for official activities authorized by the Peace Corps Act, the logo cannot be used on Volunteer Web sites.

7.4 Cultural Sensitivity

The thoughtful and accurate insights that Volunteers convey in their communications with others can contribute substantially to bringing to the United States a better understanding of other countries. However, given the broad access to Volunteer-posted material on the Web, both in their country of service and elsewhere, Volunteers should remain culturally sensitive with respect to the material they post to any Web site. Volunteers should be reminded that people in their host countries and members of the U.S. public may make inferences about the Peace Corps or the Volunteer's country of service based on the material a Volunteer posts to a Web site. Volunteer-posted material on the Web should not embarrass or reflect poorly on the Peace Corps or the countries where Volunteers serve.

7.5 Safety and Security

As a safety precaution, Volunteers must not include on their Web sites information about their precise living location or those of other Volunteers, as well as information about the location of events to be attended by a large number of Volunteers. For example, Volunteers who live in remote areas should use care before placing the name of their towns or villages on their Web site and, instead, should refer to the general area of the country where they live. For their own protection, it is advisable not to provide information about Volunteers' personal possessions. Volunteers should also be aware of the risk of identity fraud and other security concerns connected with the posting of any personal information about themselves, family members and others on Web sites.

7.6 Publication Policies

Consistent with Peace Corps' policy regarding publications, Volunteers may not accept payment for anything they write or photograph that appears on the Web. Articles, manuals, teaching materials, and other work-related products developed in connection with Peace Corps service and/or financed by Peace Corps funds are considered part of the public domain and may not be copyrighted or used for personal gain. Volunteers should be advised that posting materials to the Internet, which they have not authored or created, may violate U.S., host country, or other applicable copyright laws.
Subsection D: Use of Peace Corps IT Equipment by RPCVS

8.0 PURPOSE

Subsection D sets out the policies and mandatory guidelines for the use of Peace Corps-provided IT equipment by Returned Peace Corps Volunteers (RPCVs).

9.0 POLICIES

9.1 Scope of Use of Agency Computers

Peace Corps provides "RPCV computers" to the Career Resource Centers located at each Regional Recruitment Office (RRO) to enhance their ability to serve RPCVs. RPCV computers are set up especially for RPCVs and are not connected to the Agency staff computers. The RPCV computers will permit RPCVs to have access ONLY to the Internet, Microsoft Office, and a local office printer. No other Agency system or network resources will be provided.

9.2 Restriction on Use of Staff Computers

Agency staff are prohibited from making their staff computers available to RPCVs, and RPCVs are prohibited from accessing the staff computers. Calls for technical support for RPCV computers and printers should be reported to the Helpdesk by the RRO staff only.

9.3 Responsibilities

9.3.1 The RRO staff shall:

(a) Ensure that the Mandatory Guidelines for RPCVs are made available to each RPCV (see Attachment C) and that each RPCV completes and signs the RPCV Computer Usage Form (PC-2050) (See Attachment B);

(b) Manage computer access by RPCVs in accordance with Peace Corps policies set out in this subsection;

(c) Assign a local computer account to each RPCV. The generic account shall have the format of "RPCV-XXX." "XXX" is the three letter code identifying a particular Regional Office. For example, RPCV-CHI is the account assigned to the Chicago Office's RPCV computer. Note that, for RROs with more

than one RPCV computer, the format will be RPCV-XX1, RPCV-XX2, etc, to differentiate among the multiple RPCV computers.

(d) Create a password for the office's computer that is consistent with the Agency's password policies in Manual Section 542, Peace Corps IT Security Policies and Procedures. Notwithstanding MS 542, the passwords shall be changed once every six months by the office's technical support staff. The RRO staff shall not give a password to the RPCV until he or she has completed and signed the RPCV Computer Usage Form (See Attachment B); and

(e) Report any violations of policy by following the procedures in Attachment B of MS 542.

9.3.2 RPCVs shall:

(a) Complete and sign the RPCV Computer Usage Form (Attachment B) before accessing the RPCV computer;

(b) Read and comply with the Mandatory Guidelines for RPCVs set out in Attachment C;

(c) NOT, under any circumstances, use Agency staff computers; and

(d) NOT connect the RPCV computer or network to any non-Peace Corps organization.

10.0 EFFECTIVE DATE

This manual section shall take effect on the date of issuance.