United States Department of Agriculture
Research, Education, and Economics

ARS ❑ NIFA ❑ ERS ❑ NASS

Policies and Procedures

Title: Use of Information Technology Resources

Number: 253.4.v.2

Date: December 7, 2011

Originating Office: Office of the Chief Information Officer, ARS

This Replaces: P&P 253.4 dated September 3, 1999, April 19, 2002

Distribution: All REE Employees

This P&P defines acceptable and unacceptable uses of information technology (IT) resources such as computers telephones, E-mail, facsimile machines, cellular telephones and Internet services.

Table of Contents

1. Introduction

Agencies provide Research, Education, and Economics (REE) employees with information technology (IT) resources (e.g., PCs, E-mail, telephones, facsimile machines, copiers, office equipment, Internet access, etc.) to support mission objectives and enhance the efficient and effective delivery of services to agency customers. This P&P describes appropriate use of these resources and establishes conditions under which employees may use IT resources for non-Government purposes.

2. Authorities

- Departmental Regulation (DR) 3300-001, Telecommunications & Internet Services
- Departmental Regulation (DR) 3180-001, Information Technology Network Standards
- Departmental Regulation (DR) 1495-001, New Media Roles, Responsibilities, and Authorities
- Federal Information Security Management Act (FISMA) of 2002
- Office of Management and Budget (OMB) Circular A-123, "Internal Control Systems"
- Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
- 5 C.F.R. PART 2635 Standards of Ethical Conduct for Employees of the Executive Branch

3. General Policy

3.1 Introduction

IT resources may only be used for authorized purposes. However, "limited personal use of Government office equipment by employees during personal time is considered to be an 'authorized use' of Government property", according to DR 3300-001, Telecommunications & Internet Services and Use, dated March 23, 1999. In the REE agencies, "limited personal use" is use that involves minimal additional expense to the Government, is performed on the employee's personal time, and does not interfere with the mission or operations of an agency. DR 3300-1 is located at URL: http://www.ocio.usda.gov/directives/doc/DR3300-001.pdf .

Employees are required to abide by this policy, all system specific Rules of Behavior, other rules and regulations, and be responsible for their own personal and professional conduct. The Standards of Ethical Conduct state "Employees shall put forth honest effort in the performance of their duties" (5 CFR Section 2635.101 (b)(5)). The Standards of Ethical Conduct is located at URL: http://www.usoge.gov/laws regs/regulations/5cfr2635.aspx. These regulations remain in effect during telework and other alternate work site arrangements.

Supervisors have the management authority and responsibility to ensure the appropriate use of resources within their organizations. This includes IT resources and official employee time. As such, employees should consult with their supervisors regarding authorized use of IT resources and interpretation of this P&P. The privilege to use Government office equipment for non-Government purposes may be revoked or limited at any time by supervisors or other appropriate agency officials.

3.2 Acceptable Personal Use

Employees are permitted limited use of Government office equipment for personal needs if the use does not interfere with official business and involves minimal additional expense to the Government. This limited personal use of Government office equipment should take place during the employee's personal time, such as before or after duty hours or lunch periods.

Personal use of Government office equipment is limited to situations where the Government is already providing equipment or services and the employee's use of them will result in only minimal additional expense to the Government. This would include normal wear and tear or the use of small amounts of electricity, ink, toner, or paper.

3.3 Unacceptable Personal Use

Employees are required to conduct themselves professionally in the workplace and to refrain from using Government office equipment for activities that are inappropriate. Unacceptable personal use of Government IT resources includes:

- Any use that could generate more than minimal additional expense to the Government.

- Any use that could cause congestion, delay, or disruption of service to any Government system or equipment. For example, the forwarding of "chain" e-mails, e-mailing greeting cards, downloading or streaming of non-sanctioned video, sound or other large file attachments that can degrade the performance of the entire network.

- Activities which are illegal, inappropriate, or offensive to fellow employees or the public. Examples include pornography, hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

- Any use for commercial purposes or "for-profit" activities such as outside employment or to support a personal private business activity (e.g., consulting for pay, sales, or administration of business transactions, sale of goods or services).

- 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.

4. Internet

4.1 Acceptable Personal Use

Acceptable use of the Internet during employee personal time includes:

- Accessing the Employee Personal Page or the Thrift Savings Plan to check balances or make changes.
- Communicating with a volunteer charity organization.
- Looking at vacancy announcements.
- Collecting information for personal travel or other such personal activities.

4.2 Unacceptable Personal Use

Unacceptable use of the Internet includes:

- The creation, downloading, viewing, storage, or copying of sexually explicit or sexually oriented materials.
- The creation, downloading, viewing, storage, copying, or transmission of materials related to gambling, weapons, terrorist activities, and any other illegal or prohibited activities.
- Using the Internet for personal "for-profit" activity.
- Streaming media programs which may cause system or network congestion such as Real Player, Windows Media Player, or others in which the function is to view Internet video or listen to Internet radio. This activity is prohibited unless specifically approved to conduct official Government business. Listening to live radio via the Internet for non-work related purposes is prohibited.
- Posting Agency information to external news groups, bulletin boards, chat rooms, 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.

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

- The unauthorized acquisition, use, reproduction, transmission, or distribution of computer software or other material protected by national and international copyright laws, trademarks, or other intellectual property rights.

- Peer-to-Peer (P2P) programs that allow the participation in file sharing or file swapping activities. P2P software is frequently used for the illegal downloading of music and video files. It may also provide Internet phone connectivity or allow people to communicate from their PC's to a telephone. The following list provides examples of prohibited P2P software by category. This software is prohibited unless specifically approved to conduct official Government business:

  Instant messaging/Telephony:

AOL Instant Messenger	Yahoo Messenger	Skype
MSN Messenger	Windows Messenger	

  File Sharing:

BearShare	Gnutella	Napster
Bit Torrent	Kazaa	PC Anywhere
Edonkey	Limewire	Timbuktu
EMule	Morpheus	WinMX

4.3 Social Networking Sites

The use of Social Networking sites such as YouTube, Facebook, Twitter, etc. is becoming ever increasingly popular. USDA may block access to some of these sites due to the potential security related risks they may introduce. Additional information regarding social networking sites should be deferred to the ARS, Information Staff, phone number 301-504-1663. ARS policies and procedures for using and communicating via social media (new media) and social networking tools are described in ARS P&P 113.5.

5. E-mail

5.1 Acceptable Personal Use

Acceptable E-mail messages include:

- Occasional personal messages.

- Inquiries about your salary, insurance, retirement, or other employee benefits.

5.2 Unacceptable Personal Use

Unacceptable use of E-mail includes:

- The transmission of "junk mail" such as chain letters, hoaxes, advertisements, solicitations, or other unauthorized or inappropriate messages.

- The transmission of threatening, sexually explicit, obscene, harassing, intimidating, abusive, or offensive material.

- The transmission of messages in support of "for profit" activity.

- The transmission of email messages related to gambling, weapons, terrorist activities, and any other illegal or prohibited activities.

- The transmission of confidential or sensitive information by email, unless protected by Departmental approved encryption.

- Unauthorized Government wide or Agency wide broadcast messages.

- The use of abusive or objectionable language.

6. Telephone Equipment and Services

6.1 Acceptable Personal Use

The use of Government telephone systems (including Government issued cellular telephones and calls over commercial systems which will be paid for by the Government) are in place for the conduct of official business or limited personal use as outlined above in General Policy. Calls may be made using Government-issued wireless phone service when land-line phones are not readily available and the call is of reasonable duration and frequency. The use of cellular technology at the expense of the Government does not preclude the user from having the responsibility for inventory control, billing, and accountability.

Employees may make the following personal calls at Government expense:

- Brief daily calls to locations within the local commuting area to check the condition of

your spouse, children, or other family member.

- Calls to notify family, doctor, etc., when an employee is hurt on the job.
- Calls to advise family of a change in schedule or to make alternate transportation or child care arrangements.
- Calls to locations within the local commuting area that can be reached only during working hours, such as local Government agencies or physicians.
- Calls to schedule emergency home or car repairs.
- While traveling on Government business, a brief call to residence (but not more than an average of one call per day).
- Emergency calls using Government-issued wireless phone service when land-line phones are not readily available.

Employees may make personal calls **not** at Government expense if the call is:

- Charged to your home phone number or other non-Government number;
- Made to an 800, 877, 888, or other toll-free number;
- Charged to the called party if a non-Government number (collect call); or
- Charged to a personal credit card or prepaid calling card.

6.2 Unacceptable Personal Use

Unacceptable use includes:

- Making an unauthorized telephone call with the intent to later reimburse the Government.
- Use of “900” calls to include dialing a toll free number which will switch to a “900” call.
- Collect calls and third party calls charged to a Government number.

6.3 Safety

- Executive Order – Federal Leadership on Reducing Text Messaging While Driving was signed on October 1, 2009 which implements a Federal Government-wide prohibition on the use of text messaging while driving on official business, or while using government-supplied equipment. This Order also extends to cover Federal contractors. The entire text of the order can found at: **http://www.whitehouse.gov/the_press_office/Executive-Order-Federal-Leadership-on-Reducing-Text-Messaging-while-Driving**

- Employees must comply with state and city laws that prohibit the use of cellular telephones while operating a Government vehicle.

7. Facsimile Machines, Copiers, and Printers

7.1 Acceptable Personal Use

Examples of acceptable use of facsimile machines, copiers, and printers include:

- Occasional use of fax calls to locations within the local commuting area. Fax calls outside the local commuting area are authorized only if not charged to the Government (see Telephone section).

- Making a few photocopies.

- Using a printer to print a few pages of material.

7.2 Unacceptable Personal Use

Unacceptable use of facsimile machines, copiers, and printers include:

- Making long distance fax calls at Government expense.

- Making more than a minimal amount of photocopies, making photocopies of illegal or offensive material, or making photocopies for commercial or "for-profit" purposes.

- Using equipment for personal "for-profit" activity.

8. Sanctions for Misuse

USDA, REE will take corrective action and/or enforce the use of penalties against any user who

violates any USDA, REE, or Federal system security policy. Disciplinary actions could include the following actions, up to and including termination:

- Written reprimands.
- Temporary suspension from duty.
- Reassignment or demotion.
- Suspension of system privileges.
- Possible criminal prosecution.

9. Privacy Expectations

Each agency has the responsibility to ensure that employees are not abusing the privileges offered by this policy. The policy does not change, in any way, the agency's right to inspect equipment when there is evidence or a strong suspicion that an employee is abusing this policy.

Employees do not have a right to, nor should they expect, privacy while using any Government office equipment at any time. To the extent that employees wish their private activities remain private, they should avoid using agency-owned office equipment or information resources, such as computers, cell phones, tablet computers, the Internet, E-mail, photocopiers, or facsimile machines, for their personal use.

By using Government office equipment employees consent to disclosing the contents of any files or information maintained or passed through Government office equipment. This consent is final and irrevocable. Employees may not rely on any statements or informal policies purporting to provide you with any expectation of privacy regarding communications on this system, whether oral or written, by your supervisor or any other official, except USDA's Chief Information Officer. Any use of Government communications resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

System managers employ monitoring tools to detect improper usage. At any time, the Government may for any lawful Government purpose monitor, intercept, search, and seize any communication or data transiting or stored on this information system. Electronic communications may be disclosed within an agency to employees who have a need to know in the performance of their duties. Agency officials, such as system managers and supervisors, may access any electronic communications.

10. Summary of Responsibilities

10.1 Supervisors

- Counsel employees and monitor the use of IT resources to ensure those resources are being used appropriately.

- Immediately notify the servicing Employee Relations Specialist when they are made aware of potential misuse of Government IT resources.

- Ensure all employees complete all security awareness and other IT related mandatory training.

10.2 Employee Relations Specialists

- Determine whether misuse indicated is based on appropriate law, rule, regulation, or agency policy.

- Conduct an inquiry/investigation into the extent of the misuse of IT resource(s).

- Provide advice and guidance on appropriate disciplinary action.

10.3 Employees

- Ensure that personal use of IT resources is limited to personal time, does not interfere with official business, and involves minimal additional expense to the Government.

- Notify their immediate supervisor if they have reason to believe IT resources are being used for other than authorized purposes.

- Complete all security awareness and other IT related mandatory training.

10.4 Contractors, Collaborators, Consultants, Volunteers

- Ensure that personal use of IT resources is limited to personal time, does not interfere with official business, and involves minimal additional expense to the Government.

- Notify their Contracting Officer's Technical Representative (COTR) if they have reason to believe IT resources are being used for other than authorized purposes.

- Complete all security awareness and other IT related mandatory training.

11. Glossary

C.F.R. Code of Federal Regulations.

Information Technology. The hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal Government to accomplish a Federal function, regardless of the technology involved, whether computers, telecommunications, or others.

Information Technology (IT) Resources. Computers, computer peripherals, hardware, software, printers, telephone equipment and services, copiers and facsimile machines, electronic mail, and the Internet, owned, leased, or otherwise in the possession of the REE agencies.

Investigation. A formal examination and evaluation of relevant facts to determine whether misconduct has taken place or, if misconduct has already been confirmed, to assess its extent and determine appropriate action.

Minimal Additional Expense. An employee's personal use of Government office equipment is limited to those situations where the Government is already providing equipment or services, 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, ink, toner, or paper.

Peer-to-Peer (P2P). Refers to file sharing applications that enable computers connected to the Internet to transfer files to each other, such as Morpheus and BitTorrent.

Personal Use. An activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.

Approved:

_____ _____

Paul R. Gibson, Chief Information Officer Date
Office of the Chief Information Officer