SMG 3140.1

FDA STAFF MANUAL GUIDES, VOLUME III - GENERAL ADMINISTRATION

PERSONNEL

ETHICS AND LABOR MANAGEMENT RELATIONS

FDA POLICY ON USE OF GOVERNMENT ELECTRONIC EQUIPMENT AND SYSTEMS

Transmittal Number: 99-17 -- Date: 01/29/1999

1. PURPOSE

This policy authorizes and promotes appropriate and reasonable personal use of Government electronic equipment and systems by Food and Drug Administration (FDA) employees, on their own time, as a means to enhance their knowledge of and capabilities in using the equipment and systems in performing official duties. This Staff Manual Guide supersedes FDA Staff Manual Guide 2720.1, "Proper Use of Government Automatic Data Processing (ADP) Resources."

2. BACKGROUND

The Department of Health and Human Services' (DHHS) policy on improving the quality of work life for its employees states that Agencies should increase their investment in workplace learning, to include the development of knowledge and skills that employees need to achieve strategic goals and objectives, etc. Use of electronic equipment and systems provides employees access to, among other things, the World Wide Web and the Internet. Through the personal use of electronic equipment and systems, employees will develop competence in the effective use of technology for job-related tasks. In addition, since the Agency pays one flat fee for all Internet access, there is no additional cost for individual access or use.

3. SCOPE

This policy applies to all FDA employees; electronic equipment and systems used in Government offices, at home, in remote work sites, etc.; and associated procedures and technologies. Examples of equipment and systems include, but are not limited to, personal computers (PCs), printers, modems, the Internet, E-mail, and word processing software.

4. POLICY

FDA employees are authorized to use Government electronic equipment and systems for appropriate and reasonable personal use as long as such use:

- is appropriate under the Government's Standards of Ethical Conduct
- meets the Agency's security requirements
- does not incur additional cost to the Government
- does not stop, interrupt, or interfere with official Government business
- enhances an employee's skills in using such equipment and systems
- is conducted on the employee's personal time
- is not for an employee's personal financial gain

This policy is consistent with existing DHHS and other Federal Agency policies.

5. DEFINITIONS

Compensation: Compensation can be in the form of time or money. An employee is "compensated" for his or her time if he or she receives or earns regular pay, overtime pay, compensatory time, credit time, etc., for the time spent using Government electronic equipment and systems covered under this policy. Compensation includes time worked that will be credited towards an "Any 80" tour of duty.

Corrective action: An administrative corrective action is initiated by a supervisor in response to inappropriate conduct or behavior. A corrective action can range from an oral discussion with an employee to the employee's removal from Federal service. The action initiated will be determined on a case-by-case basis and will depend on the seriousness of the employee's misconduct, the actions proposed and/or taken in other parts of the

organization for similar misconduct, and the employee's past record of discipline, among other factors.

Employee: All employees as described in Titles 5 and 42 of the United States Code (e.g., General Schedule employees, Wage Grade employees, members of the Senior Executive Service [SES], Staff Fellows, Visiting Scientists, Experts, Consultants, Members, etc.), members of the Public Health Service Commissioned Corps employed by the FDA, contract personnel, etc.

Equipment and systems: This policy covers the use of any equipment or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes computers, ancillary equipment, software, firmware, and related resources (e.g., personal computers (PCs), modems, printers, the Internet, World Wide Web, etc.). This policy does not specifically cover copy machines, fax machines, mail meters, cellular phones, pagers, etc.

Excessive use of equipment and systems: For the purpose of this policy, "excessive use" means use which is not reasonable or "misuse." For example:

- An employee uses the Government electronic equipment and systems for personal use during her lunch break. One hour beyond her lunch break, the employee realizes that she is still using the equipment and systems for personal use. The employee must request 1 hour of leave, which may or may not be approved. In this case, the supervisor may take corrective action for the employee's violation of this policy and/or failure to secure leave approval in advance.

- An employee consistently requests leave, in advance, to use the Government electronic equipment or systems for personal use during his or her regular work hours.

- An employee stays late one evening to use the Government electronic equipment or systems for personal use and, as a result, calls in sick because he is too tired to come to work the next day.

- An employee shares a personal computer with his office mate. However, every day during his lunch break, the employee uses the computer for personal use. As a result, his office mate cannot access the computer to conduct official Government business.

Misuse: For the purpose of this policy, "misuse" means improper or incorrect use. For example:

- o personal use of the Internet while the user is being paid to conduct Government work

- o inappropriate use of the Internet to conduct activities like sending E-mail messages containing racial slurs or sending proprietary or trade secret information to a friend, or accessing Web sites containing sexually explicit or violent material

- o use of the computer's word processing, database, or spreadsheet software to support an employee's outside business where personal gain is intended or occurs

- o loading personal banking software onto the Government owned computer to conduct personal banking transactions

- o using Government computers or software to lobby Congress. (Refer to Appendix A, section II. THE "DON'TS," subsection e)

- o using Government computers or software to create and/or distribute chain letters

Own time or personal time: Any time an employee is not being compensated by the Federal Government is his or her own or personal time under this policy. For example: before and after the employee's official work schedule, during a lunch break, on weekends, etc.

Personal business: Activities that are purely personal in nature and which do not result in the employee's personal financial gain. Employees may not conduct a personal "business" using the Government electronic equipment and systems as part of an outside activity that will result in their personal financial gain. (Refer to Appendix A, section II. THE "DON'TS.")

Personal financial gain: For the purpose of this policy, "personal financial gain" means that the employee's activity is intended to or actually results in receipt of funds from the activities conducted using Government electronic equipment and/or systems. For example:

a. An employee has an authorized outside activity whereby he provides computer training services in turn for monetary compensation. That employee may not use Government electronic equipment and/or systems to conduct those activities (e.g., he may not use Government equipment and/or systems to advertise his services, produce bills for his services, prepare/print training materials, conduct the actual training, etc.).

b. An employee may not use the Government electronic equipment or systems to buy or sell stocks and/or bonds, transfer mutual fund Individual Retirement Accounts (IRA) accounts, etc.

c. An employee who has a private medical or law practice, an accounting, real estate, or other business may not prepare or store patient or client records, billing notices, spreadsheets, documents related to the practice or business, etc., on Government electronic systems.

d. An employee who owns property that is rented, may not prepare leases, correspondence, tenant documents, spreadsheets, etc., related to the rental properties.

Unauthorized use: An "unauthorized" use of Government electronic equipment and systems is any use that is in conflict with this FDA policy. For example: personal use that results in additional costs to the Government, violates the Standards of Ethical Conduct, violates laws or regulations regarding copyrighted materials, inappropriately releases proprietary or trade secret information, is done for the personal financial gain of the employee, interferes with the Government's work, etc.

Use Restricted: Offices and Centers may designate "special systems" or equipment within that Office or Center as "use" restricted (i.e., official use only). Examples of systems that may be "use" restricted are: Good Laboratory Practices (GLP), Good Manufacturing Practices (GMP), Petition Review Systems, etc. Types of equipment that can be "use" restricted are all equipment addressed in this guide (e.g., personal computers or workstations, modems, etc.).

6. RESPONSIBILITIES

A. Offices and Centers:

1. **must** publicize, in writing, any deviation (supplementation or further restrictions) from this Agency policy to their employees. In addition, a copy of the Office or Center modified policy must be provided to the Division of Ethics and Labor Management Relations.

2. **must** comply with the terms and conditions of the applicable union-management collective bargaining agreement and **must** contact the Division of Ethics and Labor Management Relations for guidance **prior** to publicizing or issuing any deviation (supplementation or further restrictions) from this Agency policy to their employees.

3. may identify, in writing, organizations or individuals who are authorized to obtain products or services over the Internet, etc., at additional costs

to the Agency, where such costs are "authorized and approved" **in advance** and when the need for such products or services is for official Government business.

B. Office and Center Information Resource Managers:

1. should assess the availability and accessibility of their equipment and systems and the appropriateness of expanding or restricting their use under this policy.

2. may, at the direction of their respective Office or Center directors, restrict the use of Government electronic equipment and/or systems beyond the FDA policy by designating equipment and systems as "use restricted" or "for official use only" for reasons such as: maintaining system security and integrity, resource constraints, system overload, limited network capacity, small disk space, limited equipment availability, proprietary information content, or when personal use could compromise the system.

3. may impose restrictions on the activities using Government electronic equipment and systems due to resource constraints or other reasons (e.g., game playing, loading software, etc.). **Refer to Responsibilities, sections (a) 1 and 2 of this Staff Manual Guide for procedural requirements.**

4. may expand this policy to include electronic equipment and/or systems not currently covered by this policy (e.g., copy machines, fax machines, etc.). Employees will be notified of any expansions in writing and, absent such written supplementation, employees are to presume they do not have authorization to do so. **Refer to Responsibilities, sections (a) 1 and 2 of this Staff Manual Guide for procedural requirements.**

5. must remove all sensitive data from electronic equipment prior to issuing it to an employee for personal use at home (Please refer to guidance published by FDA's Chief Information Officer).

6. must ensure that appropriate WEB-based and standard virus protection software is installed on computers where employees have Government Internet accounts or approved access to the Government LAN.

7. should monitor, review, audit, intercept, access, and disclose all activities using Government electronic equipment and systems. This includes, but is not limited to: all documents, spreadsheets, and messages that are created, stored, received, or sent and all Internet

inquiries made over Government electronic equipment and/or systems for any purpose (personal or official).

8. should disclose the content of inappropriate E-mail messages, spreadsheets, word processing documents, and Internet site inquiries to an employee's immediate supervisor for corrective action. The disclosure may be made without the employee's permission.

9. should approve or disapprove employee requests to install personal software or download software from the Internet to Government computers. Consideration should be given to system integrity, resource requirement conflicts, software licensing issues, and ISA standard desktop configuration conflicts.

C. Supervisors:

1. will allow employees to use Government electronic equipment and systems for appropriate and reasonable personal use within the intent of this policy.

2. must ensure that employees refrain from inappropriate use of electronic systems and initiate corrective action for an employee's inappropriate use of Government electronic equipment and systems.

3. must be knowledgeable of their Center or Office implementation guidance for this FDA policy.

4. can and should restrict an employee's use of Government electronic equipment and systems if his or her personal use conflicts with FDA policy, (e.g., use is excessive, interferes with official Government business, is inappropriate, etc.). The Division of Ethics and Labor Management Relations will assist supervisors in preparing written notification to employees on such restrictions.

D. Employees:

1. must follow Agency security policies and procedures when using Government electronic equipment and systems for official and personal reasons. This includes following Agency policies intended to safeguard "non-public" or "trade secret" information, files, passwords, etc.

2. must be knowledgeable of special requirements for accessing, protecting, and using data, including Privacy Act materials, copyrighted materials, procurement-sensitive data, etc.

3. should have no expectation of privacy when using Government electronic equipment and systems.

4. must adhere to any restrictions (e.g., game playing, installing or downloading software, etc.) on the personal use of Government electronic equipment and systems imposed by respective Offices and Centers due to resource constraints or other reasons.

5. will not use Government electronic equipment and systems in any way that might jeopardize FDA equipment, computer systems, or data files. For example, employees must follow appropriate procedures when downloading files from the Internet to avoid virus infiltration on Agency equipment or systems.

6. will request approval from the Office or Center information resource manager or Information Management Council (IMC) representative before installing personal software or downloading software from the Internet to Government computers.

7. will allow co-workers priority access to equipment and systems for conducting official Government business. The conduct of official Government business will always take priority over personal use or access.

8. must be aware that all Internet communications, via Government systems, will identify them by their complete Internet address, including the "FDA.GOV" domain. Employees using Internet communications for personal use must make it clear that the E-mail, etc., is not being used for official business and does not represent Agency activities.

9. must be aware of and inquire about additional costs associated with their personal use of electronic equipment and systems which may be incurred by the Agency and must refrain from activities that will incur such costs.

10. must ensure that only authorized personnel, as described in this Staff Manual Guide, section 5 DEFINITIONS, subsection "Employee," have access to and use of Government electronic equipment and systems (i.e., an employee's family members are not authorized to use Government electronic equipment and systems).

E. The Division of Ethics and Labor Management Relations (DELMR):

1. will advise supervisors on taking corrective actions and ensuring that the employee's due process rights are protected should corrective, disciplinary, or adverse action be initiated.

2. will answer questions from employees and supervisors about the use of electronic equipment and systems under this policy.

3. will answer questions from employees and supervisors regarding administrative matters related to this policy.

4. will assist Offices and Centers in any required union negotiations relating to this policy.

7. PRIVACY

Except as exempted by laws including the Freedom of Information and Privacy Acts, Executive Orders, or regulations, information electronically created, stored, and/or transmitted with Government-owned or leased facilities is public information and should be treated as such. The non-exempted information is available for public viewing, even if created in an employee's "personal" computer storage area, largely through the Freedom of Information Act (FOIA). Examples of information that may be made public are an employee's personal E-mails, files, and/or Internet inquiries made using Government electronic equipment and systems.

APPENDIX A - THE DO'S AND DON'TS

1. THE "DO's"

Employees may practice using Government electronic equipment and systems on their own or personal time to enhance their skills in using such equipment and systems.

a. In summary, employees may use Government electronic equipment and systems, on their own or personal time, to:

- send E-mail messages to friends or relatives to announce special events, obtain or provide information, etc.

- send E-mail messages to children at college or to a spouse who is away from home on a business or personal trip

- search for car prices or stock quotes, browse online sales catalogs, find information on vacations

- purchase airline tickets, clothes, music, books, etc., using their own (non-Government) credit cards and assuming all personal risk and

liability. However, employees may not purchase stocks, bonds mutual funds, etc.

- read newspapers, magazine articles, trade journals, etc.
- make airline, hotel, or car rental reservations
- explore the World Wide Web
- prepare a job application or resume and send it via E-mail on their own time.
- participate in on-line chat rooms available on the Internet. However, employees must make it known that their comments are their own and do not represent the views or opinions of FDA. Although they make this fact known, employees are still identified by their name and "fda.gov." **Employees are cautioned** that participation in conversations containing chat that violates the standards of ethical conduct or this policy is inappropriate and may result in corrective action. Employees may not participate in any chat room that will result in harm to FDA's reputation, compromise proprietary information, or will involve additional cost to the Government.
- send personal E-mail messages to friends. However, FDA employees should check with their friend before sending an E-mail to verify that the friend's agency has a policy that allows this activity.

b. Employees will use personally owned supplies and materials (e.g., paper, diskettes), when using Government equipment for personal use.

c. Employees should take precautions when accessing World Wide Web sites. Web browsers (MS Internet Explorer, Netscape, etc.) leave "footprints" that provide a trail of all site visits. Owners of Web sites record visitor information including names of visitors and Government agency. Employees who access a Web site from the Government system will be identified by name and "fda.gov."

d. Employees must consult with their Office or Center information resource manager or Information Management Council (IMC) representative (or his/her designee) before installing software to a Government computer.

e. Employees must consult with their Office or Center information resource manager or Information Management Council (IMC) representative (or his/her designee) before downloading files (e.g., free

software/plug-ins, RealAudio, Shockwave, Adobe Acrobat, games, screensavers, etc.) from the Internet to a Government computer. Care should be taken to avoid resource requirement conflicts, software licensing issues, and ISA standard desktop configuration conflicts, etc. Employees must protect the integrity of the Government computer system and ensure that they do not download virus infected software WEB-based and standard virus protection software must be installed on the computer.

f. Employees must follow FDA security policies and procedures, Standards of Ethical Conduct, DHHS Standards of Conduct, etc. Guidance can be obtained from the FDA Intranet, supervisors, Office or Center information resource managers, the Division of Ethics and Labor Management Relations, etc.

g. Employees must follow the established procedures for their organization. Employees should address questions or concerns about the rules established by their Office or Center regarding the implementation of this policy through the chain-of-command in their organization. Immediate supervisors are the first point of contact. Office and Center information resource managers and the Division of Ethics and Labor Management Relations can also assist.

h. Employees should address technical or procedural questions (i.e., how do I download a file from the Internet?) to their immediate supervisors or their information resource manager. Employees should also refer to their Office or Center implementation guidance for this FDA policy.

2. THE "DON'Ts"

As employees and members of the FDA community, conduct, including the use of the Internet via FDA electronic systems, reflects on the Agency's reputation. Therefore, inappropriate use of the Internet can adversely impact the Agency, and employees will be held accountable for any misconduct associated with the implementation of this policy. Employees MUST NOT VISIT SITES THAT VIOLATE THE STANDARDS OF ETHICAL CONDUCT OR THIS AGENCY POLICY.

a. In summary, employees may not use the Government electronic equipment and systems to:

- conduct an outside activity that will result in the employee's personal financial gain, (e.g., to prepare leases for property the employee owns and rents; to draft a book that the employee intends to publish and sell; to keep records of sales activities for

Tupperware, cosmetics, etc. [e.g., Mary Kay, Avon]; spreadsheets of income earned from an outside activity, medical or law practice, accounting or real estate business, etc.).

- purchase stocks, bonds, mutual funds, etc., using Government electronic equipment and systems

- produce materials or E-mails that would be disseminated to the public, a member of Congress, etc., to gain support for or defeat legislation in Congress

- solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non job-related solicitations

- create and/or distribute any offensive or disruptive messages, images, or documents. (e.g., messages, images, or documents that contain violent or sexually explicit comments or graphics, racial slurs, gender-specific comments, or any other comment or graphic that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin, or disability)

- upload (send) or download (receive) copyrighted materials, trade secrets, proprietary or other non-public information, or similar materials

- install personal software or download software from the Internet to Government computer equipment without requesting and receiving prior written approval through the chain of command (including the Office or Center information resource manager).

- create and/or distribute chain letters

- use special access privileges to view, alter, announce, or distribute the information of another user without proper authorization

- send **personal** notes, messages, announcements, etc., to an Agency-wide, Office-wide, Center-wide, or other organizational distribution. For example, employees may not:

  - ❖ send an Office-wide announcement of an upcoming community event in which FDA has no official involvement (e.g., 4th of July celebration activities, political elections, etc.)

  - ❖ send a Center-wide announcement of an upcoming personal "yard sale"

- ❖ send an Agency-wide E-mail announcing a home or car for sale

- ❖ send a message to a distribution list developed by the employee or on the employee's organization's system that does not comply with or support Agency programs as required by the Department of Health and Human Services (DHHS) Standards of Conduct

b. Employees may not process personal banking transactions from the Government PC whether at home, in the office, or at a remote work site. Personal PC banking requires additional encryption software provided by the bank. FDA will not be responsible for losses occurring from breaches of the security or integrity of those transactions.

c. Employees will not use Government electronic equipment and systems to gain access to or distribute material that is inappropriate or that may be offensive to co-workers or the public (e.g., sexually explicit or violent material).

d. Although an employee may feel that co-workers have a right to know sensitive information about another co-worker, employees may not transmit gossip, personal, or confidential information about another employee via Government electronic equipment and systems. Employees should consult with their supervisor on the matter immediately. Every employee has a right to privacy and those rights may be violated by inappropriately sharing the information. In addition, supervisors are responsible for maintaining a safe work environment for all employees. Depending on the nature of the information, the supervisor may want or need to take action.

   There may be limited occasions when it is acceptable to transmit personal information about a co-worker, with his or her prior approval, via E-mail. Employees should first check with their supervisors and their Office or Center information resource managers. Examples may include: the birth of a child, the death of a family member, wedding or retirement celebration information, etc.

   Protecting the employee's privacy is an obligation that employees and supervisors must honor.

e. Employees may not use Government electronic equipment and systems to produce materials designed to support or defeat legislation in Congress (e.g., legislation impacting Federal employee pay raises or other benefits, FDA regulatory matters, etc.). The appropriations bill prohibits the use of appropriated funds for lobbying activities. This includes the prohibition of using funds, or equipment purchased with

appropriated funds, to produce materials that would be disseminated to the public, a member of Congress, etc., and that are designed to support or defeat legislation in Congress.

f. Employees may not use Government electronic equipment to produce documents that support or oppose union activities such as: using a Government owned PC to create and print a notice about a union meeting that will be posted on an appropriately designated bulletin board. The Federal Labor Relations Statute (5 USC Chapter 71) and case law prohibit employees and union organizers from using Government equipment and materials (e.g., computers, E-mail, etc.) for internal union business or union organizing purposes.

g. Employees may use Government electronic equipment and systems to prepare grievance-related documents under the FDA Dispute Resolution System on their own time if authorized by the Office or Center implementation guidance. However, employees may not use Government-owned copy equipment to duplicate any documents in reference to a grievance. Employees should refer to FDA Instruction 771-1 dated April 14, 1998.

h. Employees may not use official time to prepare or send job applications unless they receive prior approval from their supervisor and only under limited circumstances.