ADMINISTRATIVE COMMUNICATIONS SYSTEM
U.S. DEPARTMENT OF EDUCATION

DEPARTMENTAL DIRECTIVE

Distribution:
All U. S. Department of Education Employees

Approved by: ___/s/_____
Michell Clark,
Assistant Secretary for Management

Personal Use of Government Equipment and Information Resources

Table of Contents

For technical questions concerning information found in this directive, please contact Rob Selvage via e-mail or on 202-245-6568.

Supersedes OCIO: 1-104 “Personal Use of Government Equipment” dated 03/12/2004.

I. Purpose

The purpose of this U.S. Department of Education (the Department) policy is to clarify the circumstances under which employees may use government equipment and information resources for other than official business. The Standards of Ethical Conduct require that each employee use government equipment and information resources only for "authorized uses." It is within the discretion of agency management to determine what is "authorized use" and what is not. This directive establishes what is "authorized use" and what is "unauthorized or prohibited personal use" of government equipment and information resources.

II. Authorization

The authorization for this directive is 5 C.F.R. 2635.101(b)(9) and 5 U.S.C. § 301.

III. Applicability

This policy applies to all employees of the Department. The policy also applies to contractors and employees of contractors performing work for the Department to the extent the signed contract between the Department and the contractor provides that the requirements within this directive apply to the contract.

IV. Definitions

A. Department Equipment and Information Resources

For the purpose of this directive, Personal Use of Government Equipment and Information Resources, includes the use of equipment and information resources as defined by OMB Circular A-130. This includes facsimile machines, computers (including laptops), photocopiers, telephones, printers, wireless devices, electronic mail, and electronic services. This directive does not cover cell phone usage or the use of government-issued telephone calling cards. The use of cell phones is covered in a separate ACS Handbook, OCIO-13, Handbook for Telecommunications. For questions not addressed in the Handbook for Telecommunications, please contact the Director, Network Services in the OCIO.

For the purpose of this directive, Personal Use of Government Equipment and Information Resources, does not address the use of penalty or franked mail. Penalty and franked mail is the subject of U.S. Code Title 39, Chapter 32. Under no circumstances may penalty or franked mail be used for any purpose other than official Department business.

B. Electronic Services

For the purpose of this directive, electronic services includes use of electronic mail in the Department, electronic mail over the Internet, use of computers, wireless devices, and other electronic services provided through the EDNet, services accessed through the Internet such as ListServs, file transfer protocol (ftp), or search services.

C. Personal Use

For the purpose of this directive, personal use refers to activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.

V. Policy

While ready access to current information and data is important to accomplishing the Department's mission, the Department is committed to maintaining a workplace that is free from unlawful hostility and harassment. While the Internet is a valuable information resource, it contains a wide spectrum of material on a vast array of subjects, some of which are inappropriate to the workplace. In providing Internet resources to employees, the Department balances these competing needs and priorities.

The Department also recognizes the need for efficient use of employee time and Department resources; therefore, the Department permits occasional personal use of government equipment and information resources, including facsimile machines, computers, photocopiers, telephones, printers, wireless devices, electronic mail, and electronic services, provided that such use:

- Incurs only a negligible additional expense, if any, to the Department.
- Does not impede that employee's or other employees' ability to do their jobs.
- Occurs during off-duty hours (off-duty hours are the periods of time when an employee is not expected to be working, such as during a lunch break or before and after scheduled work hours), whenever possible; and
- Is not for the purpose of generating income for the employee or another individual (i.e., the employee is not using the equipment in connection with an initiative intended to make money).

However, under no circumstances may an employee use government equipment and information resources to engage in any activity that is illegal or otherwise expressly prohibited—for example, political activity or lobbying activity prohibited by law. In addition, the use of government equipment constitutes consent to the Department's monitoring of the equipment's use.

The following are examples of authorized and unauthorized personal uses of Department equipment and information resources, including electronic services. This is not a comprehensive list and is intended only to illustrate how the Department's policy will be implemented. When terms such as "short," "few," and "brief" are used in the examples below, they mean that any personal use of government equipment and information resources described has a minimal impact on the Department. Common sense applies to all such terms.

A. Examples of Authorized Personal Use

Each example assumes that the employee is otherwise complying with this policy in that the use does not interfere with work; is done during off-duty hours, if possible; incurs only a ***negligible*** expense to the Department; and is not for the purpose of generating income for the employee (i.e., the employee is not using the equipment or information resource in connection with an action intended to make money).

- Using electronic mail to ask a co-worker to join you for a social event.
- Using the Internet to read news stories or other information of personal interest.
- Using electronic mail to ask co-workers if they can recommend a physician or plumber and to respond to a co-worker's request for a recommendation.
- Using electronic mail on the Internet to correspond with an overseas friend.
- Using electronic mail to contact your child's school and make arrangements for a conference.
- Photocopying a short document.
- Using the printer to make a small number of copies of your resume.
- Faxing an emergency note to your child's school.
- Using the computer and printer to prepare a short letter or resume.
- Using TDD/TTY or other devices to communicate with individuals with disabilities who cannot be reached by other means.
- Making brief telephone calls within the local commuting area (a local commuting area includes the location from which the employee regularly commutes);

- Using the telephone to make brief long-distance calls that are charged to your long-distance company rather than to the government. (It is never permissible to charge personal long distance phone calls to the Department.).
- Using the telephone to make alternative child care arrangements if your child becomes ill.
- Using the telephone to notify your spouse or childcare provider that you will be working late.
- Sending and receiving brief emails from friends and relatives.
- Reviewing your Thrift Savings Plan account.
- Using the Internet to research items of personal interest.

B. Examples of Impermissible Use

Each example illustrates an activity that is illegal or impermissible.

- Using LEXIS, Westlaw, or any other electronic fee-per-use service, for anything other than official business.
- Installing a game on any computer on EDNet.
- Fundraising, unless the fundraising is consistent with the Combined Federal Campaign Regulations (see 5 C.F.R. Part 950).
- Political activity prohibited by the Hatch Act (see 5 C.F.R. Parts 733 and 734).
- Representing personal opinions, or engaging in another activity, that implies incorrectly that the employee is acting on behalf of the Department.
- Distributing and/or asking to receive materials in violation of the copyright laws.
- Gambling such as football pools, harassing, or other illegal activities.
- Viewing, transmitting, making and/or causing anyone to receive sexually explicit, indecent or obscene materials.
- Selling, advertising, or promoting a product or service.

- Lobbying prohibited by 18 U.S.C. 1913 and other statutes.
- Using the computer to prepare an article for which the employee will be compensated.
- Using the computer and printer to write a book.
- Using electronic mail to advertise a rental property.
- Using the photocopier to copy a ***long document***, such as an entire cookbook.
- Using the printer to make numerous copies of your resume.
- Using the Internet to do research for your outside consulting job.
- Using the EDNet fax service to invite friends to a political event.
- Using electronic mail to solicit funds for a local charity, such as selling or buying Girl Scout cookies.
- Incurring government charges for long distance telephone calls for other than official business.
- Using electronic mail to notify anyone of your availability for consulting work.
- Using the telephone to make or receive private business calls.
- Remotely accessing the Department's network in order to use the Department's Internet access for non-official purposes. (The Department cannot be used as an alternative to a commercial Internet service provider.)

C. Examples of Permissible Use Only During Off-Duty Hours

Some uses are not illegal or unethical but are, nevertheless, inappropriate to be done during working hours. The list of authorized personal use examples above assumes that the actions can, in most cases, to be done during off-duty hours, but in some circumstances need to be done during the normal work day and do not consume an inordinate amount of time. The examples cited below illustrate activities that should not be done during working hours but are authorized personal uses if done on personal time.

- Playing solitaire, bridge, hearts, or any other game on the computer.

- Having a leisurely conversation with a friend on the telephone.
- Filling out a long job application.
- Writing a lengthy personal letter using electronic mail.

D. Policy to Filter Inappropriate Internet Material

It is the policy of the Department to provide employees with appropriate Internet access to facilitate research, learning, and the accomplishment of the Department's mission. In so doing, the Department exercises sound judgment in identifying suitable and worthwhile material for general access. Certain material contained in the Internet, such as pornography, is not required to achieve the agency's mission and, moreover, could create a hostile workplace environment. Consequently, it is the Department's policy to filter such material from general workplace access. In those rare instances in which an employee has a bona fide need to access such material in order to accomplish the Department's work, authorized personnel from the Office of the Chief Information Officer (OCIO) may disable such filters for the employee at the request of the Senior Officer or designee for the office making the request.

E. Categories of Filtered Internet Materials.

The following categories of materials are filtered from individual access.

- **Adult Material**: Adult Content - Sites that display full or partial nudity in a sexual context, but not sexual activity; erotica; sexual paraphernalia; sex-oriented businesses such as clubs, night clubs, and escort services; and sites supporting online purchase of such goods and services.
- **Adult Material**: Lingerie and Swimsuit - Sites featuring pictures that include alluring or revealing attire.
- **Adult Material**: Nudity - Sites featuring pictures of exposed breasts or genitalia.
- **Adult Material**: Sex - Sites depicting or implying sex acts.
- **Adult Material**: Sex Education - Sites dealing with topics in human sexuality, including sexual technique, sexual orientation, cross-dressing, transvestism, transgenderism, multiple-partner relationships, and related issues.
- **Bandwidth PG**: Peer-to-Peer File Sharing – Sites that provide client software to enable peer-to-peer file sharing and transfer.

- **Gambling** - Sites dedicated to promotion of, or participation in, wagering, gambling, casinos or lotteries.

- **Games** - Sites dedicated to games, gaming, game tips, game downloads, interactive games, and multiplayer games.

- **Illegal Activities** – Sites providing instructions on performing illegal activities or acquiring illegal items.

- **Information Technology**: Hacking - Sites that provide information about or promote illegal access to or use of computer or communication equipment, software, or databases.

- **Information Technology**: Proxy Avoidance – Internet sites allowing content retrieval on behalf of a user with the intent of obscuring the user's identity.

- **Information Technology**: URL Translation Sites - Sites that offer online translation of URLs. These sites access the URL to be translated in a way that bypasses the proxy server, potentially allowing unauthorized access.

- **Internet Communication**: Web Chat - Sites providing interactive communication services such as Web chat or bulletin boards.

- **Internet Communication**: Web-based Email - Sites providing interactive electronic-mail service.

- **Productivity PG**: Advertisements - Sites that provide advertising graphics or other ad content files.

- **Productivity PG**: Instant Messaging - Sites that enable instant messaging.

- **Racism and Hate** – Sites advocating intolerance or hatred of a person or group of people.

- **Society and Lifestyles**: Personals and Dating – Sites dedicated to personals, dating, escort services or mail order marriages.

- **Security PG**: Malicious Web Sites - Sites that contain code that may intentionally modify end-user systems without their consent and cause harm.

- **Security PG**: Spy ware - Sites or pages that download software that, without the user's knowledge, generates http traffic (other than simple user identification and validation).

F. Consent to Monitoring

The use of any government equipment and/or information resource covered by this directive constitutes consent by the user to the Department's monitoring of use activity at all times. Department computer systems and related equipment are intended for the communication, transmission, processing, and storage of official United States government or other authorized information only. Department computer systems are subject to monitoring by OCIO to ensure proper functioning of equipment and systems, including security devices and systems; to prevent unauthorized use and violations of statutes and security regulations; to deter criminal activity; and for other similar purposes. Use may be monitored, intercepted, recorded, read, copied, captured and disclosed by appropriate officials. There is no right to privacy for users. Use (authorized or unauthorized) of Department systems constitutes consent to monitoring, interception, recording, reading, copying, capturing or disclosure by appropriate officials.

If monitoring of Department computer systems reveals possible evidence of violations of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring of Department computer systems reveals violations of security regulations or unauthorized use, employees who violate security regulations or make unauthorized use of Department computer systems are subject to appropriate disciplinary action.

VI. Responsibilities

A. Employee Responsibilities

Employees are responsible for ensuring that government equipment and information resources are used in an efficient manner with an emphasis at all times towards conserving government property and resources. Employees are responsible for using government equipment and information resources in a competent and professional manner. For example, large files and large volumes of mail delivered over the Department's local network and saved in shared electronic storage (servers) can burden the system and cause extra costs to the government, through slowed transmission of information and by necessitating additional electronic storage facilities. Examples of excessive personal use of government equipment are downloading multimedia files or saving mail with large attachments, sending announcements with unnecessary graphics, photocopying multiple copies of personal items, or printing large documents for personal use. Employees are also under an obligation not to use large amounts of paper, toner, or other office supplies for personal use. Employees should contact their supervisors if there is any question whether an intended use of government equipment is permissible.

All have an obligation to report misuse of electronic services or government equipment or information resources.

An employee who violates this directive may be subject to administrative action in accordance with Personnel Management Instruction 751-1, Discipline and Adverse Actions, including Appendix A: Table of Penalties for Stated Offenses.

B. Supervisory Responsibilities

Supervisors who become aware that an employee is using government equipment and information resources in a manner that costs the Department more than a "negligible" amount (for example, printing more than a few pages of research from the Internet), or for profit (e.g., consulting or teaching job), have an obligation to take necessary steps to ensure the employee complies with this directive, including initiating appropriate disciplinary action and/or limiting employee access to the computer or to electronic services.

C. OCIO Responsibilities

OCIO monitors Department computer systems to ensure proper functioning of equipment and systems including security devices and systems; to prevent unauthorized use and violations of statutes and security regulations; to deter criminal activity; and for other similar purposes. Use may be monitored, intercepted, recorded, read, copied, captured and disclosed by OCIO or other appropriate officials.

D. Senior Officer or his/her Designee Responsibilities

If the Principal Office's management determines that an employee needs access to normally filtered Internet materials to accomplish a mission-related need, the Senior Officer or his/her designee may request that access for specific individual(s) along with the business justification by contacting the OCIO Help Desk at helpdesk@ed.gov

OCIO reserves the right to deny access to any site that is deemed to be a security risk.

E. Contractor Responsibilities

The Department and the contractor sign a contract to be the legally binding agreement for work to be performed for the Department. It is the expectation of the Department that a contractor using government equipment and information resources will comply with this directive, to the extent it is required to do so by the provisions of the legally binding contract.

F. Contracting Officer Responsibilities

A Contracting Officer who observes or is notified that a contractor has not complied with the requirements of this directive is responsible for informing the contractor's corporate management and determining the appropriate remedy.

VII. Procedures and Requirements

If an employee or contractor misuses the Department's information technology infrastructure in a way that results in interference of normal network operations, such as sending and receiving very large volumes of mail, uploading and downloading very large files, or downloading any software or electronic files from outside the Department without ensuring that reasonable virus protection measures are in place, the Department can place restrictions on the user's access to, or use of, government equipment.

The same standards of civility and decency apply to electronic mail as to other forms of communication. The use of profanity, racial or ethnic slurs, sexually harassing language, and any other such language is as inappropriate on electronic mail as it is elsewhere in the office and will not be tolerated. This policy applies to all communications made using Department equipment—regardless of whether the communication is official or, where permitted under this policy, personal. This is particularly important because employees' Internet addresses all contain the designation ed.gov, indicating that the message is coming from a computer within the Department. Employees should remember that "deleted" electronic messages may still be recorded by tapes maintained by the Department and that computers maintain a limited record of Internet sites visited by anyone using that computer.

Any attempt to circumvent any of the Department's security mechanisms, either from within or outside the Department's facilities, constitutes a violation of its information security policies. Such violations will be addressed in accordance with the Handbook OCIO-01, Handbook for Information Assurance Security Policy.

Any suspected security threat or breach of the Department's automation and information resources, or any violation or attempted violation of its information security policies, must be immediately reported to an employee's supervisor or to appropriate security personnel or to a contractor's Contracting Officer's Representative or the Contracting Officer, as appropriate.

Please see the following Department policy documents, all found on ConnectED, for more specific information:

- OM-01, Handbook for Classified National Security Information;
- OCIO-01, Handbook for Information Assurance Security Policy;
- OM 4-114, Physical Security Program;

- OCIO-13, Handbook for Telecommunications;
- OIG:1-102, Cooperation With and Reporting to the Office of the Inspector General;
- PMI 751-1: Discipline and Adverse Actions;
- PMI 751-1, Appendix A: Table of Penalties for Stated Offenses.