



DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS

Program Statement

OPI:	OMITS
Number:	2420.4B
Supersedes:	2420.4A (9/30/03)
Date:	February 21, 2008
Subject:	Email and Internet Use

1. **PURPOSE AND SCOPE.** To provide guidelines for acceptable use of the Internet and Email within the DC Department of Corrections (DOC).

2. **POLICY.** It is the policy of the DOC to provide electronic systems as tools to meet employee's programmatic needs as well as to expedite business communications, reduce paperwork, and automate routine office tasks, thereby increasing productivity and reducing costs.

3. **APPLICABILITY**
 - a. This policy applies to all full or part-time employees, contractors, consultants or volunteers who are authorized to use DC Government resources and who have been provided with a user account and all other users of DC Government IT resources. No employee shall have any expectation of privacy as to Internet and Email use.

 - b. DOC has software and systems in place that can monitor and record all Internet and Email use. DOC security systems are capable of recording (for each and every user) each web site visit, each chat, newsgroup or Email message, and each file transfer into and out of its internal network. DOC reserves the right to do so at any time. DOC managers shall have access to Internet and Email activity and use pattern audits.

 - c. All DC government and DOC policies relating to intellectual property protection, privacy, misuse of government resources, sexual harassment, data security and confidentiality apply to employee conduct on the Internet and when using Email.

4. **NOTICE OF NON-DISCRIMINATION.** In accordance with the D.C. Human Rights Act of 1977, as amended, D.C. Official Code §2.1401.01 et seq., (Act) the District of Columbia does not discriminate on the basis of race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, gender identity or expression, familial status, family responsibilities, matriculation, political affiliation, genetic information, disability, source of income, or place of residence or business. Sexual harassment is a form of sex discrimination that is also prohibited

by the Act. Discrimination in violation of the Act will not be tolerated. Violators will be subject to disciplinary action.

5. **PROGRAM OBJECTIVES.** The expected results of this program are:

- a. To ensure consistent use and proper management of Email and the Internet for the conduct of official government business in a manner that complies with federal and local statutory authorities, DC government use policies and this directive.
- b. Employees shall understand the proprietary nature of all information created, sent or received via DOC's Email System.
- c. Email and Internet Policy shall be incorporated into employee pre-service, annual In-service training and periodic orientation processes.

6. **DIRECTIVES AFFECTED**

a. Directives Rescinded

PS 2420.4 Internet Use (6/25/99)

b. Directives Referenced

1) PS 5140.2 Information Security Program (9/15/03)

7. **AUTHORITY**

a. DC Law 12-175, Act 12-239

b. DC Code Section § 24-211.02 [Formerly §24-442]

c. OCTO 0001 Internet Access and Use Policy (8/1/01)

d. OCTO 0002 Email Use Policy (8/1/01)

8. **STANDARDS REFERENCED**

a. American Correctional Association (ACA) 2nd Edition Standards for Administration of Correctional Agencies: 2-CO-1F-07, 2-CO-1F-09, 2-CO-1F-10 and 2-CO-1F-15.

b. American Correctional Association (ACA) 3rd Edition Standards for Adult Local Detention Facilities: 4-ALDF-7D-17.

9. RESPONSIBILITIES

- a. The Deputy Director shall ensure agency adherence to DOC Internet and Email policy and procedures.
- b. The Office of Management Information and Technology Services (OMITS) is responsible for the day-to-day control of Internet information provided or accessed by DOC employees, and to ensure Email services are used for internal and external communication that serve legitimate government functions and purposes. OMITS is also responsible for maintenance of the related, resident infrastructure for Email and Internet access by DOC employees.
- c. The Office of Public Affairs (OPA), in conjunction with OMITS, shall ensure that information DOC makes available on the Internet shall be appropriate for public access and editorially suitable.
- d. Employees shall adhere to the provisions of this directive and sign an acknowledgement of receipt of its issuance.

10. ALLOWABLE USES OF INTERNET AND EMAIL

- a. Communication and information exchange directly related to the mission, charter or work tasks of a DC government agency.
- b. Research and information exchange in support of advisory, standards, analysis, and professional development activities related to the user's DC government duties.
- c. Announcement of DC government laws, procedures, policies, rules, services, programs, information or activities.
- d. Administering or applying for contracts or grants for DC government programs or research.
- e. Other governmental administrative communications not requiring a high level of security.
- f. Communication and information exchange for professional development, to maintain currency of training or education or to discuss issues related to the Internet user's DC government activities.
- g. Advisory capacity, standards, research, analysis and professional society activities related to the user's governmental work tasks and duties.
- h. Inmates shall never be provided or allowed access to the Email or Internet system.

11. SPECIFICALLY PROHIBITED USES OF INTERNET AND EMAIL

- a. Any purpose which violates a federal or DC government law, code, policy, standard or procedure.
- b. Private business or personal gain, including commercial advertising.
- c. Access to and/or distribution of indecent or obscene material, child pornography, fraudulent information, harassing material, materials in violation of DOC sexual harassment policy or racial information.
- d. Transmission of information or statements that contain profane language, pander to bigotry, sexism or other forms of prohibited discrimination, or can in any way be construed as intending to harass or threaten another individual.
- e. Interference with or disruption of the network and/or associated users, services or equipment.
- f. Unapproved broadcast or chain letter-type emails in which an email message, regardless of its content or purpose, is sent or forwarded to a group list or multiple email accounts.
- g. Disruption, obstruction, or burden of network resources.
- h. Dissemination or solicitation of information that would reflect negatively on or damage the public image of the DC government or its agencies.
- i. Any activity with religious or political purposes.
- j. Any unauthorized purchases.
- k. Transmission of sensitive (e.g., confidential) information unless protected by an approved encryption mode.

12. SENSITIVE EMAIL TRANSMISSION

- a. Sensitive information that is considered privileged under an attorney-client relationship, information subject to the Privacy Act, proprietary information, or other information which must be protected from unauthorized disclosure, shall be protected during transmission as follows:
 - 1) The sender shall be certain that the recipient is properly authorized to receive and view the information.
 - 2) The sender shall clearly identify and mark sensitive (e.g., confidential) messages immediately below the message header (i.e., the Subject, Data, From, and To lines) as:

SENSITIVE/CONFIDENTIAL INFORMATION
(or)
[ATTORNEY/CLIENT PRIVILEGED INFORMATION]
Do Not Release To Unauthorized Persons.

13. **PROTECTED HEALTH INFORMATION (PHI).** PHI must be clearly identified immediately below the message header as Protected Health Information. In addition the following confidentiality statement shall be incorporated into all Email transmissions that contain PHI.

PRIVACY/CONFIDENTIALITY NOTICE (PHI):

The information in this transmission contains protected health information in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This message is intended only for the use of the individual to which it is addressed and contains information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. Violation of Privacy Rules may result in civil and criminal penalties consistent with CFR 164.512(k)(5)(iii). If you are not the intended recipient, please contact the sender by email, fax or phone and destroy all copies of the original message.

14. **PROCEDURES**

a. General

- 1) DOC users, including employees and supporting consultants/contractors, are acting as representatives of DOC and shall not engage in any activity or transmit any communication that would reflect unfavorably on DOC or be deemed inappropriate by DOC, conflict with any laws, regulations, or policies of any local jurisdiction in any material way.
- 2) Use of DOC resources knowingly for illegal activity shall be grounds for immediate dismissal. Complete cooperation shall be given to all legitimate law enforcement agencies.
- 3) In the event that access privileges are misused or abused, supervisors or sponsors of contractors/consultants shall request removal or suspension of access privileges for the individuals involved. Such requests shall be made in writing to the OMITS Administrator.
- 4) If it is determined that the misuse or abuse constitutes cause for discipline, actions shall be consistent with provisions of the applicable

District Personnel Manual (DPM) and the collective bargaining agreement:

- a) Chapter 16 General Discipline and Grievances,
 - b) Chapter 8 Probationary Employees,
 - c) Chapter 9 Excepted Service Employees,
 - d) Chapter 38 Management Supervisory Service, or
 - e) Chapter 18, Part I Employee Conduct.
- 5) Email and Internet access is for business use, therefore messages are to be courteous, professional, and businesslike. Posting or transmitting material that is obscene, hateful, harmful, malicious, threatening, hostile, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable is not business use and is prohibited.
 - 6) Monitoring and filtering software shall be installed by the OMITS, only, to ensure that the desired environment for productive work is provided.
 - 7) Files that are downloaded from the Internet or email attachments must be scanned with virus detection software provided by OMITS before installation and execution. Appropriate precautions shall be taken to detect viruses and to prevent their spread.
 - 8) The truth or accuracy of information on the Internet and in Email is to be considered suspect until confirmed by the originator or by a separate reliable source.
 - 9) Solicitation of non-DOC business or any use of the electronic media for personal gain is prohibited.
- b. Internet Access
- 1) Access to the Internet requires written approval from the requestor's supervisor and the Administrator (OMITS), is accomplished through LAN workstations, and requires the installation of additional software. Requests explaining the need for access by specific individuals are forwarded through supervisory channels to the Director, OMITS.
 - 2) The Internet does not guarantee the privacy or confidentiality of information. Sensitive DOC material may not be transmitted over the Internet unless such transmission is properly encrypted and pre-approved by senior DOC leadership.
 - 3) DOC provides access to the Internet through the District of Columbia Wide Area Network (DCWAN). Alternate connections to DOC's internal network are not permitted unless authorized beforehand, in writing, by OMITS.

- 4) Unless otherwise noted, all software on the Internet shall be considered copyright protected work. Employees are prohibited from communicating, disseminating, or printing any copyrighted materials in violation of applicable copyright laws. In consideration of DOC's grant of Internet access to employees, such employees agree to indemnify and save harmless DOC from and against any and all claims, demands, liabilities, causes of action, losses, damages and costs (including attorneys fees) arising out of or related to employee's violation of applicable laws or this policy in connection with such employee's use of the Internet access that was granted.
- 5) All data transmitted becomes the property of DOC. DOC has the right to access, review, copy, and delete any data sent, received, or stored, and reserves the right to disclose this information to any party, whether inside or outside DOC, that DOC deems appropriate, insofar as it is consistent with any applicable local law, HIPPA or any other federal law, regulations, copyrights or licenses.

c. Email Use

- 1) Email addresses identify the organization that sent the message; therefore Email is equivalent to letters sent on official letterhead.
- 2) Users of the DOC Email system are expected to follow the same business rules as used with other written correspondence in terms of addressees, distribution, use of supervisory and administrative chains, and organizational structures.
- 3) Storage of large numbers of Email messages is discouraged, as large numbers of Emails will negatively impact system performance.

d. OMITS shall:

- 1) Serve as DOC liaison with the District's Office of the Chief Technology Officer (OCTO).
- 2) Provide state-of-the-art Internet access and service for authorized use by DOC employees, selected outside entities, and consultants/contractors that DOC has deemed, in its sole discretion, should be granted access to the Internet via the DOC network.
- 3) Design, maintain, and upgrade DOC's Internet and Email infrastructure.
- 4) Provide technical assistance to LAN administrators and users.
- 5) Install and configure web browser software on computer workstations upon approval of requests for Internet access. Maintain appropriate user

and Transmission Control Protocol/Internet Protocol (TCP/IP) for Internet activation and monitoring.

- 6) Maintain the master files listing DOC employees, contractors, and consultants who currently have authorized access and maintain historical files of former employees authorized access in the past. Maintain original signed Internet Use Policy Acknowledgement forms.
 - 7) Ensure that security procedures are current, understood, and that DOC is in compliance with established security policy.
 - 8) Install monitoring and filtering software on DOC Networks that is capable of recording (for each and every user) each web site visit, each chat room, newsgroup or Email message, and each file transfer into and out of DOC's internal networks.
 - 9) Ensure that all information technology and related records are managed in accordance with the Office of Internal Controls, Compliance and Accreditation (OICCA), Retention and Disposal of Department Records, Program Statement No. 2000.2, that no records are destroyed without proper authorization and that disposition schedules are kept current.
 - 10) Ensure that passwords are changed on a periodic basis and that DOC Email system reminds authorized Email users when it is time for them to change their Email password.
 - 11) Monitor Internet and Email use and report all suspected violations to the Deputy Director.
 - 12) Develop training programs for use by the Training Academy, Human Resource Managers, and Wardens/Administrators/Office Chiefs to orientate and train new employees and to ensure that all employees fully understand their responsibilities related to the use of the DOC Email and Internet.
 - 13) Design and maintain DOC's web site.
 - 14) Assist other DOC Offices in linking to the DOC web site and other Internet sites.
- e. Warden/Administrators/Office Chiefs shall:
- 1) Ensure that outside entities, consultants, and contractors supporting them understand and agree to adhere to the policies related to Email and Internet use, and submit original Internet Use Policy Acknowledgement forms to OMITS.
 - 2) Report all suspected violations of this policy to OMITS.

- f. The Office of Public Affairs (OPA), in conjunction with OMITTS shall:
 - 1) Serve as content manager for DOC web site.
 - 2) Evaluate, approve, and/or disapprove suggested additions and changes related to the DOC web site.
 - 3) Ensure that information released to the public represents DC and DOC concerns and that the information that DOC makes available on the Internet is appropriate for public access and editorially suitable; i.e., appropriate in terms of editorial suitability and conformity with federal and local policy and standards.
 - 4) Consults with the Office of General Counsel when necessary to determine suitability of information for DOC web site.

- g. DOC employees and other authorized users shall:
 - 1) Access Email messages for the first time in private to protect confidentiality of possibly sensitive information they may contain.
 - 2) All Internet and Email users shall sign the attached statement.
 - 3) Routinely change passwords based on the DOC automatic reminder program and maintain their passwords confidential.
 - 4) Log off and disconnect communication links when leaving workstations unattended. Failure to logout of the Internet or Email manager shall not relieve an employee of liability for misuse of Internet or Email resources by someone else.
 - 5) Treat the Email and Internet systems as if they were a shared file system, with the expectations that messages sent, received, or stored on the servers or on individual hard drives will be available for review by any authorized representatives of DOC for any purpose.
 - 6) Identify themselves honestly, accurately, and completely when participating in newsgroups or when setting up accounts on outside computer systems.
 - 7) Chat rooms and newsgroups are public forums and it is inappropriate to reveal sensitive information, inmate data, operations procedures, or any other information covered by DOC policies and procedures.
 - 8) Authorized employees, only, shall speak/write on behalf of DOC to newsgroup, the media, to analysts, or to chat rooms in a public gathering or other forums.

- 9) Follow the guidelines outlined in this directive and do not use the Internet to deliberately propagate any virus, worm, Trojan horse, or trap door program code.
- 10) Report any suspected violations of this directive to the Supervisor.


Devon Brown
Director

Attachment – Internet and Email Use Acknowledgement