
	DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	December 19, 2016	Page 1 of 13
	POLICY AND PROCEDURE		SUPERSEDES:	2420.4C May 9, 2014	
			OPI:	INFORMATION TECHNOLOGY	
			REVIEW DATE:	December 19, 2017	
			Approving Authority	Quincy L. Booth Interim Director	
	SUBJECT:	E-MAIL AND INTERNET USE			
NUMBER:	2420.4D				
Attachments:	Attachments A – Internet and Email Use Acknowledgment				

SUMMARY OF CHANGES:

Section	Change
	<i>Minor changes have been made.</i>

APPROVED:



Quincy L. Booth, Interim Director

12/19/16

Date Signed

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	December 19, 2016	Page 2 of 13
POLICY AND PROCEDURE		SUPERSEDES:	2420.4C May 9, 2014	
		REVIEW DATE:	December 19, 2017	
SUBJECT:	E-mail and Internet Use			
NUMBER:	2420.4D			
Attachments:	Attachments A – Internet and Email Use Acknowledgment			

1. **PURPOSE AND SCOPE.** To provide guidelines for acceptable use of the Internet and Email within the DC Department of Corrections (DOC).
2. **POLICY.** The DOC provides 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 and part-time employees, contractors, consultants and volunteers who are authorized to use DC Government resources and who have been provided with a user account and authorization to use of DC Government IT resources. Authorized users shall not 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 OIT monitors access to user's internet and e-mail activity. DOC managers have access to usage patterns or audit logs via a written request to the OIT Manager. Verbal or 2nd party requests will not be honored."
 - 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.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	December 19, 2016	Page 3 of 13
POLICY AND PROCEDURE		SUPERSEDES:	2420.4C May 9, 2014	
		REVIEW DATE:	December 19, 2017	
SUBJECT:	E-mail and Internet Use			
NUMBER:	2420.4D			
Attachments:	Attachments A – Internet and Email Use Acknowledgment			

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

- a. Proper use and 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. Employee understanding of the proprietary nature of all information created, sent or received via DOC's Email System.
- c. Incorporation of Email and Internet Policy shall be incorporated into employee pre-service training, annual in-service training and periodic orientation processes.

6. **DIRECTIVES AFFECTED**

- a. Directives Rescinded
PP 2420.4C Internet Use (5/9/14)
- b. Directives Referenced
1) PP 2420.2 Information Security

7. **AUTHORITY**

- a. DC Law 12-175, Act 12-239
- b. DC Code Section § 1-1403
- c. DC Code Section § 24-211.02. Powers; promulgation of rules
- d. OCTO 0001 Internet Access and Use Policy (12/15/03)
- e. OCTO 0002 Email Use Policy (10/16/07)
- f. District Personnel Manual, Chapter 8, Career Service
- g. District Personnel Manual, Chapter 9, Excepted Service

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	December 19, 2016	Page 4 of 13
POLICY AND PROCEDURE		SUPERSEDES:	2420.4C May 9, 2014	
		REVIEW DATE:	December 19, 2017	
SUBJECT:	E-mail and Internet Use			
NUMBER:	2420.4D			
Attachments:	Attachments A – Internet and Email Use Acknowledgment			

- h. District Personnel Manual, Chapter 16, General Discipline and Grievances
- i. District personnel manual, Chapter 18, Employee Conduct
- j. District Personnel Manual, Chapter 38, Management Supervisory Service
- k. Collective Bargaining agreement between The Government of the District of Columbia Department of Corrections and The Fraternal Order of Police Department of Corrections dated September 30, 2005.

8. STANDARDS REFERENCED

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

9. RESPONSIBILITIES

- a. The Office of Information and Technology (OIT) shall ensure agency adherence to DOC Internet and Email policy and procedures in conjunction with the OCTO security team.
- b. The Office of Information and Technology (OIT) 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 serves legitimate government functions and purposes. OIT is also responsible for maintenance of the related, resident infrastructure for Email and Internet access by DOC employees.
- c. The Office of Government and Public Affairs, in conjunction with OIT, 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;

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	December 19, 2016	Page 5 of 13
POLICY AND PROCEDURE		SUPERSEDES:	2420.4C May 9, 2014	
		REVIEW DATE:	December 19, 2017	
SUBJECT:	E-mail and Internet Use			
NUMBER:	2420.4D			
Attachments:	Attachments A – Internet and Email Use Acknowledgment			

- b. Research and information exchange in support of standards, analysis, advisory, 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, subject to the broadcast email requirements described below;
- d. Application for, or administration of, contracts or grants for DC government programs or research;
- e. Other governmental administrative communications not requiring a high level of security;
- f. Interagency and external broadcast correspondence that:
 - 1) Is limited to 100 recipients or fewer,
 - 2) Is not sent to the group distribution list of any other agency (except for emergency communications), and
 - 3) Does not constitute or contain (as an attachment or otherwise) any inter-agency or external bulletin, newsletter, announcement, promotional material, manual, guide, brochure, or marketing collateral, all of which must be posted on websites and not sent in group emails outside the sender's agency list.
- g. Interagency and external broadcast emails with distribution greater than 100 recipients that are authorized in advance by the Director of Communications of the Executive Office of the Mayor (EOM) or the Chief Technology Officer;
- h. Mayoral broadcast missives, upon 2 hours' notice to OCTO or with shorter notice to OCTO, in the discretion of the Director of Communications, EOM;
- i. Incidental personal purposes, provided that such use does not:
 - 1) Directly or indirectly interfere with the DC Government operation of computing facilities or electronic mail services,
 - 2) Burden the DC Government with noticeable incremental cost, or

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	December 19, 2016	Page 6 of 13
POLICY AND PROCEDURE		SUPERSEDES:	2420.4C May 9, 2014	
		REVIEW DATE:	December 19, 2017	
SUBJECT:	E-mail and Internet Use			
NUMBER:	2420.4D			
Attachments:	Attachments A – Internet and Email Use Acknowledgment			

3) Interfere with the email user's employment or other obligations to the DC Government.

j. Inmates shall never be provided or allowed access to the Email or Internet system that do not meet security requirements for DOC GED or other DOC sanctioned educational site requirements.

11. SPECIFICALLY PROHIBITED USES OF INTERNET AND EMAIL

- a. Any purpose that violates a federal or DC government law, code, policy, standard or procedure.
- b. The advertising or other promotion of any private business enterprise or activity.
- c. Transmission or solicitation 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, sexually or otherwise.
- d. Any activity with religious or political purposes outside the scope of the user's assigned and authorized governmental duties.
- e. Any unauthorized purchase.
- f. Sending email under names or addresses other than the employee's own officially designated DC government email address.
- g. Adding, removing, or modifying identifying network header information ("spoofing") in an effort to deceive or mislead recipients.
- h. Opening any "executable" email attachments (e.g., .exe, .bat, .scr, .vbs) from any source.
- i. Sending or forwarding "chain" letters, i.e., those that ask the receiver to forward the message to multiple recipients.
- j. Sending any attachment files larger than 25 megabytes (MB).
- k. Sharing organized District email lists with any person outside the District, except as required by the Freedom of Information Act, subpoena, or other compulsory process.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	December 19, 2016	Page 7 of 13
POLICY AND PROCEDURE		SUPERSEDES:	2420.4C May 9, 2014	
		REVIEW DATE:	December 19, 2017	
SUBJECT:	E-mail and Internet Use			
NUMBER:	2420.4D			
Attachments:	Attachments A – Internet and Email Use Acknowledgment			

- l. Setting email correspondence to forward automatically to an outside (non-District) address.
- m. "Broadcast" emails that do not meet the "broadcast" email requirements above.
- n. Disruption, obstruction, or burden of network resources.
- o. Unauthorized enhancements or add-on software to Outlook (e.g., animations, backgrounds, pictures).
- p. Use of non-District email services such as Yahoo or AOL on the District's computer network.
- q. Use of non-District file sharing such as (but not limited to) Facebook, Twitter, or other file or picture sharing web sites.
- r. The intentional or negligent introduction of computer viruses into any DC Government systems; agencies must prevent the introduction of computer viruses into DC government systems and must install District-standard virus-scanning software to check any software downloaded as email attachments.
- s. Transmission of sensitive (e.g., confidential) information unless protected by an approved encryption mode.
- t. Conducting government business through private e-mail accounts.

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:

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	December 19, 2016	Page 8 of 13
POLICY AND PROCEDURE		SUPERSEDES:	2420.4C May 9, 2014	
		REVIEW DATE:	December 19, 2017	
SUBJECT:	E-mail and Internet Use			
NUMBER:	2420.4D			
Attachments:	Attachments A – Internet and Email Use Acknowledgment			

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 shall not engage in any activity or transmit any communication that would reflect unfavorably or be deemed inappropriate by DOC or, conflict with any local laws, regulations, or policies.
- 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

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	December 19, 2016	Page 9 of 13
POLICY AND PROCEDURE		SUPERSEDES:	2420.4C May 9, 2014	
		REVIEW DATE:	December 19, 2017	
SUBJECT:	E-mail and Internet Use			
NUMBER:	2420.4D			
Attachments:	Attachments A – Internet and Email Use Acknowledgment			

of access privileges for the individuals involved. Such requests shall be made in writing to the Office of Information and Technology (OIT).

- 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 Career Service,
 - 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 OIT, 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 IT 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 (OIT), is accomplished through LAN workstations, and requires the installation of additional software.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	December 19, 2016	Page 10 of 13
POLICY AND PROCEDURE		SUPERSEDES:	2420.4C May 9, 2014	
		REVIEW DATE:	December 19, 2017	
SUBJECT:	E-mail and Internet Use			
NUMBER:	2420.4D			
Attachments:	Attachments A – Internet and Email Use Acknowledgment			

Requests explaining the need for accesses by specific individuals are forwarded through supervisory channels to the OIT Chief.

- 2) The Internet does not guarantee the privacy or confidentiality of information. Sensitive DOC material may not to 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 OIT.
- 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 DOC from 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, and is not protected by any privilege.

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.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	December 19, 2016	Page 11 of 13
POLICY AND PROCEDURE		SUPERSEDES:	2420.4C May 9, 2014	
		REVIEW DATE:	December 19, 2017	
SUBJECT:	E-mail and Internet Use			
NUMBER:	2420.4D			
Attachments:	Attachments A – Internet and Email Use Acknowledgment			

d. OIT 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 up to date master files listing DOC employees, contractors, and consultants who currently have authorized access, maintain historical files of former employees authorized access in the past, and 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 Accreditation and Compliance (OAC) procedures, *Retention and Disposal of Department Records*, PS 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 Email system reminds authorized Email users when it is time for them to change their Email password.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	December 19, 2016	Page 12 of 13
POLICY AND PROCEDURE		SUPERSEDES:	2420.4C May 9, 2014	
		REVIEW DATE:	December 19, 2017	
SUBJECT:	E-mail and Internet Use			
NUMBER:	2420.4D			
Attachments:	Attachments A – Internet and Email Use Acknowledgment			

- 11) Monitor Internet and Email use and report all suspected violations to the Deputy Director for Management Support.
 - 12) Update and maintain DOC's web site.
 - 13) 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, agree, and adhere to the policies related to Email and Internet use, and submit original Internet Use Policy Acknowledgement forms to OIT.
 - 2) Report all suspected violations of this policy to OIT.
- f. The Office of Government and Public Affairs, in conjunction with OIT shall:
- 1) Serve as content manager for the 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 laws and regulations.
 - 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.

DISTRICT OF COLUMBIA DEPARTMENT OF CORRECTIONS		EFFECTIVE DATE:	December 19, 2016	Page 13 of 13
POLICY AND PROCEDURE		SUPERSEDES:	2420.4C May 9, 2014	
		REVIEW DATE:	December 19, 2017	
SUBJECT:	E-mail and Internet Use			
NUMBER:	2420.4D			
Attachments:	Attachments A – Internet and Email Use Acknowledgment			

- 3) Routinely change passwords based on the DC Government/OCTO Web Mail programs and maintain their passwords confidentially.
- 4) Log off and disconnect communication links when leaving workstations unattended. Failure to logout of the Internet or Email applications 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 web conferences (such as but not limited to WebEx), or other conference forums or when setting up accounts on outside computer systems.
- 7) Refrain from chat rooms and other public forums that reveal sensitive information, inmate data, operations procedures, or any other information covered by DOC policies and procedures.
- 8) Speak/write on behalf of DOC to a newsgroup, the media, to analysts, or to chat rooms in a public gathering or other forums only when authorized.
- 9) Follow the guideline outlined in this directive and does 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 their Supervisor.



DC Department of Corrections Email and Internet Use Policy Acknowledgement

I, _____, have received a written copy of the DC Department of Corrections' (DOC) Email and Internet Use Policy and Procedure 2420.4. I fully understand the terms of this policy and agree to abide by them.

I realize that the DOC's security software may, for management and security purposes, record the Email and Internet address of each site that I visit and may maintain a record of network activity in which I transmit or receive any kind of file.

I acknowledge that any message I send or receive will be recorded and stored in an archive file for management's use.

I acknowledge that violation of this policy could result in suspension of my access to the Email and Internet, discipline, termination or criminal prosecution.

_____ Name	_____ Signature	_____ Date
_____ Witness	_____ Signature	_____ Date