

Department of Mental Health
TRANSMITTAL LETTER

SUBJECT Electronic Mail (Email) Acceptable Use Policy		
POLICY NUMBER DMH Policy 686.1	DATE May 27, 2003	TL# 24

Purpose. To establish standards for the proper use of DC government-provided electronic mail (email) services. Also, the name of Information Systems Management has been changed to Information Services.

Applicability. Applies to all employees DMH-wide (DC Community Services Agency, St. Elizabeths Hospital, and the Mental Health Authority); contractors who are authorized to use DC government-owned equipment or facilities; volunteers who are authorized users of DC government resources and have been provided with an associated email account; and all users of DC government Information Technology (IT) resources.

Policy Clearance. Reviewed by affected responsible staff and cleared through appropriate Mental Health Authority offices.

Implementation Plans. A plan of action to implement or adhere to this policy must be developed by designated responsible staff. If materials and/or training are required to implement this policy, these requirements must be part of the action plan. Specific staff should be designated to carry out the implementation and program managers are responsible for following through to ensure compliance. Action plans and completion dates should be sent to the appropriate authority. Contracting Officer Technical Representatives (COTRs) must also ensure that contractors are informed of this policy if it is applicable or pertinent to their scope of work. *Implementation of all DMH policies shall begin as soon as possible. Full implementation of this policy shall be completed within sixty (60) days after the date of this policy.*

Policy Dissemination and Filing Instructions. Managers/supervisors of DMH and DMH contractors must ensure that staff are informed of this policy. Each staff person who maintains policy manuals must promptly file this policy in Volume I of the blue **DMH** Policy and Procedures Manual, and contractors must ensure that this policy is maintained in accordance with their internal procedures.

*If any CMHS or DMH policies are referenced in this policy, copies may be obtained from the DMH Policy Support Division by calling (202) 673-7757.

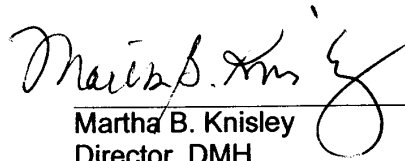
ACTION

REMOVE AND DESTROY

NONE


INSERT

DMH Policy 686.1



Martha B. Knisley
Director, DMH

Government of the District of Columbia

GOVERNMENT OF THE DISTRICT OF COLUMBIA  DEPARTMENT OF MENTAL HEALTH	Policy No. 686.1	Date May 27, 2003	Page 1
	Supersedes None		

Subject: Electronic Mail (Email) Acceptable Use Policy

1. **Purpose.** To establish standards for the proper use of DC government-provided electronic mail (email) services.

2. **Applicability.**

Applies to:

- All employees DMH-wide (DC Community Services Agency, St. Elizabeths Hospital, and the Mental Health Authority);
- Contractors who are authorized to use DC government-owned equipment or facilities;
- Volunteers who are authorized users of DC government resources and have been provided with an associated email account; and
- All users of DC government Information Technology (IT) resources.

3. **Authority.** DC Government Policy Number OCTO0002, Email Use Policy; DC Law 12-175, Act 12-239.

4. **Policy.**

4a. The District of Columbia Department of Mental Health (DMH) electronic mail system is intended for business purposes. Personal use is permissible only within reasonable limits and in accordance with the guidelines of this policy. Any authorized user who violates this policy will be subject to suspension of service and disciplinary action, up to and including termination.

4b. The e-mail system's software and hardware are DMH property; all messages composed, sent, or received on the e-mail system are and remain the property of DMH. DMH Information Services may periodically exercise its right to review, audit, intercept, access, or disclose all messages created, received, or sent.

4c. DMH reserves the right to regularly review an authorized user's e-mail records. Therefore, authorized users should have no expectations of privacy regarding e-mail messages. The contents of e-mail may be disclosed within DMH without the permission of the authorized user.

4d. DMH e-mail records are subject to disclosure to law enforcement or other third parties through subpoena or other legal processes and are subject to applicable record retention policies.

4e. DMH shall establish security precautions to protect sensitive (e.g., confidential) information from intentional, inappropriate, or accidental disclosure and protect the DC government or an individual from loss or harm.

5. General Email Guidelines and Etiquette. Authorized users:

- 5a. Shall respond to email messages in a prompt business like manner. It is unacceptable to disregard any business related email that requests a response and/or action;
- 5b. Shall write email messages in a professional and courteous tone since they are equivalent to an official letter;
- 5c. Should audit messages regularly and should delete or archive any messages that are no longer needed;
- 5d. May only use their assigned user IDs and properly licensed software. User IDs may not be shared with other persons;
- 5e. May not access or read any messages other than their own, notwithstanding DMH's right to retrieve and read any e-mail messages;
- 5f. Should ensure that they have addressed all e-mail messages to the appropriate recipients;
- 5g. May not send or forward confidential information to outside individuals or companies not authorized to receive that information, or to persons inside DMH who do not need to know the information;
- 5h. Should assume e-mail systems are not adequately equipped to protect messages considered highly sensitive, confidential, or personal regardless of encryption methods or other security precautions;
- 5i. Should be aware that communications that appear humorous to one authorized user might be offensive to another authorized user; and
- 5j. Should never download email attachments unless the email was received from a known and trusted source.

6. Allowable Uses of Email. Allowable uses of email in DMH include:

- 6a. Communication and information exchange directly related to the mission, charter, or work tasks of DMH;
- 6b. Professional development activities related to the user's DMH duties;
- 6c. Announcement of DC government laws, procedures, policies, rules, services, programs, information, or activities;
- 6d. Use in administering or applying for contracts or grants for DMH programs or research; and
- 6e. Other governmental administrative communications not requiring a high level of security.

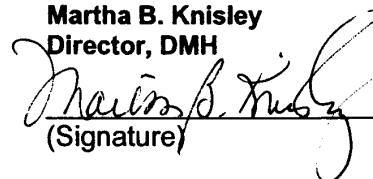
7. Prohibited Uses of Email. Prohibited uses of email in DMH are as follows:

- 7a. Any purpose which violates a federal or DC government law, code, or policy, standard or procedure;
- 7b. Any purpose not directly related to the mission, charter, or work tasks of DMH;

- 7c. Private business, including commercial advertising;
- 7d. 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;
- 7e. 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;
- 7f. Sending email under names or addresses other than the employee's own, officially designated DC government email address. Adding, removing, or modifying identifying network header information (known as "spoofing") in an effort to deceive or mislead recipients;
- 7g. Disruption, obstruction, or burden of network resources;
- 7h. Dissemination or solicitation of information that would reflect negatively on or damage the public image of the DC government or its agencies;
- 7i. Any activity meant to foster personal gain;
- 7j. Any activity with religious or political purposes;
- 7k. Any unauthorized purchases; and
- 7l. Transmission of sensitive (e.g., confidential) information unless protected by an approved encryption mode:
- (1) Sensitive information includes protected health information, information 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;
 - (2) For approved encryption modes, refer to applicable DMH information security policies, standards, and procedures;
 - (3) Sensitive (e.g., confidential) messages must be clearly identified 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 PERSONNEL." In such cases, the sender must also be certain that the recipient is properly authorized to receive and view the information.
8. **Inquiries.** Contact the DMH Information Services Helpdesk at 673-7125 if you have questions.
9. **Related References.** DMH Policy 645.1, DMH Privacy Policies and Procedures

Approved By:

Martha B. Knisley
Director, DMH


(Signature)

May 27, 2003
(Date)