DC | HEALTH
GOVERNMENT OF THE DISTRICT OF COLUMBIA

District of Columbia Department of Health **Electronic Mail Use**		**PROCEDURE 720.300** Implementing Office: Office of the Director Training Required: No Originally Issued: 1/13/2014 Revised/Reviewed: APR 26 2022 **(Second Revision)**
Approved by: LaQuandra Nesbitt MD, MPH; Agency Director	**Review by Legal Counsel:** Phillip Husband, Esq.; General Counsel	**Effective Date:** APR 26 2022 **Valid Through Date:** APR 26 2025

I. Authority	Reorganization Plan No. 4 of 1996; Mayor's Order 1997-42; OCTO Email Use Policy (5/25/2021)
II. Reason for the Policy	Electronic mail (email) is a vital tool for communicating both internally and with external stakeholders. DC Health employees have a responsibility to use email responsibly within the bounds of ethics and professional conduct. Email from DC Health employees should also be aesthetically consistent and reflect the DC Health style guide. Additionally, email is a point of vulnerability for cybercrime including fraudulent attempts to gain unauthorized access to DC Health networks and databases ("phishing"). A protocol is required to ensure that email is used appropriately for legitimate government business, reflects DC Health logos and branding, and mitigates the risk of malicious attacks.
III. Applicability	This policy applies to all DC Health employees, contractors, volunteers, interns, summer youth employees, and federal employees assigned to the District government (collectively referred to herein as "employees" or "DC Health employees.")
IV. Policy Statement	Email is part of the portfolio of the DC Health Office of Information Technology (DC Health IT). The Chief Information Technology Officer (CITO) is the accountable manager over DC Health IT.

The email system software and hardware are the property of the District government. All messages composed, sent, or received on the email system are the property of the District government. DC Health, or the Office of the Chief Technology Officer (OCTO), reserve the right to review, audit, intercept, access, or disclose messages created, received or sent. The DC Health electronic mail system is intended for District government uses only. Personal use is permissible only within reasonable limits and in accordance with the guidelines of this policy.

DC Health employees are responsible for all content in outgoing emails and ensuring that all outgoing messages reflect the highest customer service standard (see SOP 240.500 Customer Service). Examples of prohibited uses of email include, but are not limited to:

1. Any purpose which violates a federal or District government law, code, policy, standard, or procedure;
2. Private business, including commercial advertising;
3. Links to personal social media accounts;
4. 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;
5. Unapproved "broadcast" or chain letter-type emails, that are not considered DC Health government business, in which an email message, regardless of its content or purpose, is sent or forwarded to a group list or multiple email accounts;
6. Sending email under names or addresses other than the authorized user's own officially designated DC Health government email address.
7. Adding, removing, or modifying identifying network header information in an effort to deceive or mislead recipients;
8. Any activity meant to foster personal gain;
9. Any activity with religious or political purposes;
10. Copyrighted materials that belong to entities outside DC Health;

	DC Health employees are prohibited from using a personal email address to conduct government business, regardless of the intent of such an action. All emails pursuant to any government business shall be sent from the employee's assigned government email address. Any employee whose job duties include access to information protected under federal or District law is responsible for maintaining compliance with those protections and is responsible for knowing when such information may, and may not, be transmitted by email. Such information includes, but is not limited to, protected health information, and protected employee information. Managers supervising employees with access to legally protected information are responsible for ensuring that each employee in their office has access to the resources needed to determine if information may, or may not, be transmitted by email. Managers may, at their discretion, mandate training to ensure compliance with relevant laws and prevent unlawful disclosure of information. DC Health reserves the right to regularly review an authorized user's email records. Authorized users should have no expectation of privacy regarding email messages. The contents of email may be disclosed within DC Health without the permission of the authorized user. DC Health email records are subject to disclosure and applicable record retention policies. All messages shall contain an email signature consistent with the most recent version of the DC Health style guide, developed and distributed by the Office of Communications and Community Relations (OCCR).The employee may include links to DC Health official social media accounts in his/her email signature. The listed job title in the email signature shall be the employee's title of record as it appears in his/her electronic personnel record or official sanctioned external communications. All outgoing emails shall have a plain, unadorned, white background. DC Health shall cooperate fully with any investigation, within the District government, or from an external investigating authority, concerning a prohibited use of email.

	All DC Health employees will comply with mandated cybersecurity retraining from OCTO. The DC Health Director, or designee, has the authority to mandate all, or any subset of DC Health employees complete retraining in cybersecurity. DC Health employees are expected to review all incoming emails per guidance offered in OCTO cybersecurity training and not open attachments from any sender that is suspect. DC Health employees will forward all possible phishing emails to the designated OCTO address for review immediately. Any employee who opens a suspect attachment for any reason shall report the incident to OCTO and their supervisor immediately. Any employee in violation of any part of this SOP may be subject to commensurate disciplinary action.
IV. Definitions & Acronyms	**CITO-** Chief Information Technology Officer **DC Health IT-** DC Health Office of Information Technology **Email-** Electronic mail. A means or system for transmitting messages electronically (as between computers on a network). **OCCR-** DC Health Office of Communications and Community Relations **OCTO-** District of Columbia Office of the Chief Technology Officer **Phishing-** The practice of tricking internet users (as through the use of deceptive email messages or websites) into revealing personal or confidential information which can then be used illicitly
VI. Procedures	None
VII. Contacts	Chief Information Technology Officer
VIII. Related Documents, Forms and Tools	None