



State of North Carolina
Department of Public Safety
POLICIES & PROCEDURES

INFORMATION TECHNOLOGY

Division: ADMINISTRATION
Chapter: INFORMATION
TECHNOLOGY
Policy: EMAIL
ACCEPTABLE USE
Issue Date: OCTOBER 23, 2012
Revised:

I. PURPOSE

Email is a business communication tool, and users are obligated to use this tool in a responsible, efficient, and lawful manner. Although by nature Email appears to be a less formal means of communication, the same professional standards apply to Email as to other more formal written communication.

II. SCOPE

This policy applies to all employees, including permanent, contractual, and consultant employees who work for the Department of Public Safety and use the Department of Public Safety computing and networking resources. All users are expected to become familiar and comply with the guidance provided herein. Questions regarding this policy should be directed to the Department of Public Safety's Information Security Office (Statutory and/or Regulatory Authority: Statewide Information Security Manual (020121); § 147-33.110).

III. POLICY

1. Email Usage. Any Department of Public Safety Email System should be used primarily for business purposes only. Employees and the department can be held liable for illegal or improper use.
 - a. Users shall not send or forward Email containing libelous, defamatory, or obscene remarks.
 - b. Users shall not use Department Email to vent negative emotions, or to send harassing, embarrassing, indecent, intimidating, or other unethical, immoral, or unlawful material.
 - c. Users are prohibited from sending or forwarding messages that are likely to offend on the basis of race, gender, religion, national origin, sexual orientation, age, or disability.
 - d. Users may not send chain letters, junk mail, or personal files that utilize high bandwidth.
 - e. Users are not allowed to use Email for private business activities.

- f. DPS managed email systems shall retain email records for a 10 year period.
 - g. Unless authorized by DPS management, users shall not routinely use third party web mail accounts (e.g. Yahoo, Hotmail, Gmail, etc.) or other non-DPS email accounts to conduct DPS business. Users are responsible for retaining any email messages from web mail and/or personal email accounts that are used for state business. Users shall ensure that the aforementioned personal/web email messages are retained for a 10 year period.
 - h. Users shall not attempt to forge or disguise their identity when sending Email.
 - i. Users are prohibited from sending Email messages using another person's Email account unless they are a Proxy for a user that has granted them permission to send Email from their account.
 - j. Users may not utilize an unauthorized method to encrypt an Email message without first obtaining written permission to do so from the IT/MIS Section. Confidential or sensitive information shall not be transmitted via Email without the proper encryption enabled.
 - k. Confidential or sensitive information shall not be put in the subject line of an Email (e.g. social security numbers). Email users should check with their supervisors if they are unsure about what to put in the subject line.
 - l. Employees shall refrain from selecting unknown/untrusted Email links and /or opening untrusted/unexpected email attachments.
 - m. Employees are reminded that the use of Department resources, including Email, should never create either the appearance or the reality of inappropriate use.
2. Personal Use. While minimal personal use of email will be tolerated, excessive personal use of email is prohibited.
 3. Privacy. All messages distributed by any of the department's email systems shall become the property of the Department of Public Safety. Users expressly waive any right to privacy in anything they create, store, send, or receive via Email.
 4. Violations. Violations of this policy may result in revocation of privileges, restricted access to network systems, and/or other appropriate disciplinary action, up to and including dismissal. The Department of Public Safety



reserves the right to monitor all network assets, including employee Internet usage.