

SUBJECT: **ELECTRONIC MAIL (EMAIL)**

Supersedes: None; New policy
Effective: February 15, 2005
Page: 1 of 3

1.0 POLICY PURPOSE

Detroit Public Schools (DPS) is committed to protecting the integrity, confidentiality, and availability of its informational assets. This policy:

- Describes email users' responsibilities for the proper use of DPS electronic (email) service and potential consequences for failing to abide by these rules
- Ensures users are aware of what DPS deems to be acceptable and unacceptable use of email
- Informs users that by using the DPS email service the user agrees to comply with this policy and waives any right of privacy in any email they create, send, or receive using the DPS email, or store in the DPS email system
- Places users on notice that DPS can and may monitor use of email without prior notification, and that DPS reserves the right to take disciplinary action, including termination or legal action for failing to adhere to this policy

2.0 SCOPE

This policy applies to any email message that is created or received by users of the Detroit Public Schools electronic mail service. Users of DPS email are employees or business partners (i.e. contractors or vendors) who have been issued a DPS email address.

3.0 POLICY

Email is a business communication tool that is provided as a condition of employment. It is to be reviewed and used on a regular basis (i.e. communications with supervisor and other employees, to receive district wide announcements). Users are obliged to use it in a responsible, effective, and lawful manner. Although by nature email may seem to be less formal than other written communications, the same laws apply.

1. DPS email service is to be used primarily for business purposes. Uses that interfere with normal business activities are strictly forbidden.
2. Although email is meant for business, DPS allows personal use if it is reasonable, responsible, and does not interfere with work or violate the terms of this policy. However, the sending of chain letters, junk mail, jokes, and executables is strictly prohibited and could result in employee termination.
3. Users shall not use email for any for-profit business activities, operating a business for personal gain, or soliciting money for religious or political causes.

4. Users shall not use email for solicitation or to transmit or request material that could potentially embarrass DPS or for which DPS could be held liable. In particular, users are forbidden from creating, downloading, or transmitting emails that contain offensive or disruptive material concerning sexual orientation, gender, race, age, political or religious beliefs, disability or national origin, or includes material that is obscene, pornographic, or is in any way threatening, or that is racially or sexually harassing. Receipt of email containing such materials should be reported immediately to the user's supervisor. Sending of email containing such materials can cause disciplinary action.
5. Users shall not use email to send or receive commercial software or other material to circumvent licensing agreements.
6. Users shall not use email to provide unauthorized access to private or confidential information.
7. Information protected by the Family Education Rights to Privacy Act (FERPA), 20 USCS § 1232g, is not to be sent externally via email unless approved by DPS management and is sent with the body of the email and any attachments encrypted.
8. Users shall not use email to provide access to public information without following the existing rules and procedures of DPS for dissemination.
9. Technical and Information Systems (TIS) is responsible for the setting of encryption standards. Users may not encrypt any email without obtaining written permission from their supervisor and the DPS TIS Division. If approved, the encryption key(s) must be made known to DPS.
10. Users shall not use another user's email account nor should a user allow someone to use their account. If an email user believes their password has been compromised they should change it immediately using password criteria stated in DPS Policy 13.05 - Password Protection.
11. Users should report any incidents of email abuse to their managers and/or the office of the Chief Technology and Information Systems Officer (CTIO).

4.0 ENTERPRISE DISCLAIMER (Attached to every email)

This email and any attachments contain confidential and/or privileged information and are intended solely for the above-mentioned recipient(s). If you have received it in error, please notify the sender immediately by email and delete this email from your system. You must not copy, distribute, disclose, store, or take any action in reliance on it. Neither this information block, the typed name of the sender, nor anything else in this message is intended to constitute an electronic signature unless a specific statement to the contrary is included in this message.

5.0 ISSUANCE OF REGULATIONS/STANDARD OPERATING PROCEDURES

The Chief Technology and Information Systems Officer has developed regulations and/or standard operating procedures to implement this policy.

6.0 FAILURE TO COMPLY

Failure to comply with this policy and/or the corresponding regulations may result in a recommendation to the Chief Executive Officer for appropriate disciplinary action.

7.0 EXCEPTIONS

The DPS Chief Technology and Information Systems Officer must document and approve any exceptions to this policy.

8.0 AGREEMENT

I, _____ (print name) have read the Detroit Public Schools Electronic Mail (Email) policy, dated _____. I understand it and agree to abide by it.

Signed

DETROIT PUBLIC SCHOOLS
ADMINISTRATIVE REGULATION

INFORMATION SECURITY

This Administrative Regulation implements Detroit Public Schools (DPS) Policy 13.07 – Electronic Mail (Email)

1.0 Ownership

Email stored on the DPS email system, including attachments, belongs to DPS, not the individual user, and users should have no expectation of privacy as to its contents, regardless of the steps taken by the user to protect the privacy of such documents, such as using encrypted passwords. DPS reserves the right to read any email stored on the DPS email system at any time without notice to or permission of the user. It is possible that for either a criminal or civil action DPS email may be used as evidence.

2.0 Retention

The vast majority of email messages has only transitory value to DPS and should be discarded after being read. However, some messages remain useful to DPS business for a period of time because they have reference, legal, administrative, functional, or policy/programmatic (archival) value.

If you are unsure whether an email is transitory or requires a level of archiving consult with your immediate manager or records officer in helping with your decision. Messages that are not immediately deleted should be filed with related records and retained in accordance with the document retention schedule prepared by the Office of General Counsel 5/24/2002.

a. Transitory Value

Many messages are of limited value to DPS. These messages contain no documentation of decisions or information, which serves as the basis for action to be taken.

Examples include:

- Personal business unrelated to DPS business
- Electronic copies of messages previously printed or filed
- Spam (unsolicited, commercial email not directed to you individually)
- Messages to or from email distribution lists not directly relating to DPS business
- Copies of publications
- Routine requests for information or publications
- Letters of transmittal that add no information to that contained in attachments. However, it may be important to prove time of receipt.

- Informational messages that do not serve as the basis of action or decisions, such as announcements relating to holidays, charitable appeals, bond campaigns, etc.
- Received copies of messages sent from within DPS and preserved by the sender. In rare instances, it may be wise to retain a copy of the message either as proof of receipt or you lack confidence that the sender will keep the original copy.

Suggested retention is 0-30 days with no destruction notice necessary.

b. Reference Value

Messages that duplicate the official record copy or messages of limited value should be kept for a short period of time.

Examples include:

- Templates or routine updates
- Meeting agendas
- Reference materials used for analysis or document creation

Suggested retention: Indefinite. Delete when of no further use.

c. Permanent Value

Messages of enduring value that need to be kept permanently should be stored onto a network drive where backup and storage procedures are in place. Another option, however not recommended, can be to store the message onto the hard-drive of your workstation or notebook computer.

Examples include:

- **Legal Value;** messages sent from within DPS or received from outside of DPS that may help DPS successfully defend itself against litigation actions, enforce its rights, or meet other legal obligations and needs, including compliance with statutes or regulations.
- **Administrative Value;** messages that facilitate the day-to-day operations of DPS or which are sent from within DPS or are received from outside DPS in the routine course of administering programs. To the extent that the message serves as the record of distribution of important business (minutes, policy changes, etc), the message may have administrative value independent of the value of the message content.
- **Functional Value;** messages sent from DPS or received outside of DPS that are created as the result of well-defined activity (business process) with similar, if not identical, content and format, and which may be filed as a series. Includes case files, transaction files, and personnel files.
- **Policy and Programmatic Value;** messages sent from within DPS or received from outside of DPS that relate to DPS policies and programs. These messages are evidence of management decisions that affect DPS work, including the development, modification, or termination of policies and programs.

Retention periods apply to both sent and received messages. If you are the sender of a message, you have primary responsibility for discarding or

retaining the message properly. If you have received an internal (DPS) message, the sender holds the retained copy. If you receive an external message your copy of the message is the record copy.

3.0 Offensive

Emails received that can be identified as hostile or harassing information that is derogatory, defamatory, obscene, or offensive, or anything that may be perceived as harassment or disparagement based upon race, color, national origin, sex, sexual orientation, age, disability, or religious or political beliefs should be immediately deleted from your in-box and trash folders.