## 7540.05 - ELECTRONIC MAIL PROCEDURES

### Purpose:

The purpose of this procedure is to assign responsibility and provide procedures related to establishing, operating, maintaining, and accessing e-mail services.

The Superintendent or designee is responsible for providing policy and procedural guidance for establishing, operating, and maintaining the Board's E-mail services. The considerable benefits gained by Internet/E-mail to convey information quickly must be balanced by comprehensive use of risk management procedures and the adherence to the procedures below. Each user is personally responsible for protecting and properly using the user identification codes and access to their E-mail account from any workstation. If E-mail with inappropriate content is discovered, the originator's supervisor shall be informed for appropriate disciplinary actions.

A. Utilization of E-mail by District employees is strongly encouraged for communication purposes. The following are Internet E-mail technical requirements:

1. Do not open attachments from unknown people or sources.

2. When in doubt, confirm with the sender before opening any attachment.

3. If an attachment is unintentionally opened and the computer behaves strangely, contact the site technician immediately.

4. Use of the Board's E-mail for any purpose other than official District business shall be limited and shall not interfere with assigned duties.

B. Prohibited uses of the Internet and/or E-mail shall include but not be limited to the following:

1. Illegal, fraudulent, or malicious activities.

2. Partisan political activity, political or religious advocacy, or activities on behalf of organizations having no affiliation with the District, the State of Florida, the United States Government, or a bona fide professional non-profit educational organization or advocacy group.

3. Activities whose purposes are for personal or commercial financial gain which may include, but not be limited to chain letters, solicitation of business or services, gambling, or sales of personal property.

4. Unauthorized fundraising or similar activities, whether for commercial, personal, or charitable purposes, unless specifically authorized by the Superintendent or the Board.

5. Accessing, storing, processing, displaying, possessing, printing, or distributing offensive or obscene material such as pornography, hate literature, sexually offensive, or other inappropriate information.

6. Annoying or harassing another person by sending undesirable E-mail or displaying uninvited web sites or by using lewd or offensive language in an E-mail message.

7. Making racist or sexist comments or any other statements which demean a person because of his/her race, sex, sexual orientation, national origin, age, disability, color, or religion.

8. Any other usage that may create a potential legal liability for the Board or compromise the Board in any way.

9. Illegal or unethical messages, or those that are not in good taste or that may be offensive or abusive to any person or entity, such as, those containing sexually explicit or obscene messages, racial or ethnic slurs or language that could be constructed as harassing or insulting.

10. Surveys, contests, pyramid schemes, chain letters, junk E-mail, spamming, or any duplicative or unsolicited messages (commercial or otherwise).

11. Defame, abuse, harass, stalk, threaten, or otherwise violate the legal rights (such as rights of privacy and publicity) of others.

12. Advertise or offer to sell or buy any goods or services for any personal purpose.

13. Mail files that contain viruses, Trojan horses, worms, time bombs, cancelbots, corrupted files, or any other similar software or programs that may damage the operation of another's computer or property of another.

14. Harvest or otherwise collect information about others, including E-mail addresses.

15. Create a false identity for the purpose of misleading others.

16. Spoof E-mail messages.

17. High-priority E-mails are only to be used in EMERGENCY situations. The utilization of this feature increases the load on the Board's E-mail server.

18. Do not use Board E-mail to communicate with friends and family throughout the work day, except in case of emergency, and when they cannot be reached by phone.

19. Using the District E-mail to subscribe to:

    a. daily jokes

    b. daily horoscopes

    c. daily recipes

    d. vacation destination information

    e. similar items of information or amusement

C. Signature Blocks

1. E-mail messages from employees should contain the following information within the signature block:

    a. employee's name

    b. position/title

    c. building; address; phone number

2. Employees' signature blocks may not include quotes, regardless of the source (e.g., no quotes from famous historical figures, Biblical figures, or anyone else).

## Usage Restrictions:

A. Confidential information should never be transmitted utilizing e-mail.

B. Use of distribution lists can be regulated by the site administrator or a person's supervisor and are only to be used when it is necessary to convey information to every member of a group.

C. If utilizing a District-wide or building-wide distribution lists, it is the responsibility of the sender to know where the information will be sent.

D. Personal encryption of E-mail is prohibited.

E. E-mail may not include information that violate copyright restrictions.

F. Attachments in excess of 20 MB internally externally may not be transmitted. Any file transfers greater than stated must be done in an alternative manner (e.g., physical disk such as CD, FTP, etc.). Attachments that do not conform to Board procedures may not be transmitted.

## Spamming:

The Board can immediately terminate any account which it believes, in its sole discretion, is transmitting or is otherwise connected with any spam or other unsolicited bulk E-mail. Spamming or sending mail to ALL users is not acceptable unless an emergency or system maintenance notification warrants this action.

## Complaints Received Electronically:

Any incoming message containing a complaint, allegation, or improper conduct, or expression of dissatisfaction over the handling of funds or an account must be immediately brought to the site manager's attention.

## Monitoring:

The Board can monitor E-mail messages that employees send and receive. The Board makes no guarantees concerning the privacy of electronic mail. Server logs and rejected messages may be read at the Board's discretion. The Board will also cooperate with law enforcement agencies and any other source that makes a legal request for E-mail stored on the Board's servers or backup devices.

E-mail monitoring will include monitoring for the improper use of confidential data that is not to be transmitted via E-mail or any unsecured transfer method. This type of data monitoring includes Social Security numbers and bank account numbers.

## Mailbox Creation Requirements:

A. Requests from the site manager must be sent via E-mail using the "Help Desk" E-mail account or a hard copy request by mail. The following information is required to create an E-mail account.

1. Last Name – as defined on the human resources system
2. First Name – as defined on the human resources system
3. Alt-ID - to validate user as a valid District employee
4. Official School or Site Name
5. Department – as defined by Finance Division
6. Title of Employee – as defined by assigned Human Resources job code
7. Telephone Number

B. All non-employee accounts must be approved by the site manager.

## Specific Account Restrictions:

A. Each E-mail user is responsible for keeping his/her E-mail account at a manageable size.

B. All server E-mail folders except "Deleted Items", "Junk Mail", and "Sent Items" will retain email until deleted or the 50 GB overall storage limit is reached. "Deleted Items" and "Junk Mail" will be removed after thirty (30) days and "Sent Items" will be removed after ninety (90) days if not moved to a different folder.

C. If a mailbox is not maintained beyond the recommended levels, the mailbox could become corrupt or be unusable until the appropriate maintenance is implemented.

D. Maximum Size of Mailbox – 50 GB

E. Maximum Size of Attachments – 10 MB internally, 5 MB externally

F. Deletion of Mailboxes

1. The supervisor of the terminated employee is responsible for initiating the request for transferring any information from the terminated employee's E-mail to the supervisor's or designee's mailbox.
2. The terminated personnel's mailbox shall be deleted within thirty (30) days of the receipt of the termination notice from the District's Human Resources Department or upon the notification by the employee's supervisor, whichever is earlier.

G. Software used to automatically check the calendaring function cannot be set to monitor more frequently than once in every five (5) minutes.

## Retention of Electronic Mail:

Electronic messages created or received in connection with official business that is used to "perpetuate, communicate, or formalize knowledge" are considered public records and are subject to all public access and records management laws and regulations. However, not all E-mails are considered public records. It is important for employees to know the distinction between E-mails that are public records and transitory E-mail messages so they can satisfy the relevant legal requirements in all cases.

## Public Record E-mail:

## Florida's Public Records Law:

Florida's public records law, listed in F.S. Chapter 119, defines public records as:

"All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software or other material, regardless of physical form, or characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency."

The Florida Supreme Court interprets this definition to encompass all materials made or received by an agency in connection with official business which are used to perpetuate, communicate, or formalize knowledge. All of these materials, regardless of form, are open for public inspection unless the legislature has specifically exempted them from disclosure. One Florida court has held that "information stored in a computer is as much a public record as a written page in a book or a tabulation in a file stored in a filing cabinet".

## How the Law Affects You as a BPS Employee:

E-mail created or received by BPS employees in connection with official business, which perpetuates, communicates or formalizes knowledge, is subject to the public records law and open for inspection. This includes Yahoo, Hotmail, or any other commercial Email applications you might be using. It is for these reasons that BPS highly recommends you never use personal Email to conduct official District business.

## Subject Lines:

Fill in the subject line on the E-mail to help the recipient identify and file messages and to aid in the filing of OUT box messages that must be retained for the appropriate retention period. Subject lines should be as descriptive as possible.

## FRCP:

A. What is FRCP?

The U.S. Supreme Court approved on April 12, 2006 what may be the most far-reaching change for the handling of e-mails as evidence in all Federal courts. The "Amendments to the Federal Rules of Civil Procedure" (FRCP) has significant impact because, among other things, it defines what is acceptable for discovery and disclosure in legal cases.

B. How does the FRCP impact IT?

The FRCP creates an extremely broad description of what "electronically stored information" must be disclosed, places a time limit for the disclosure, and stipulates a "good-faith" test on retention schedules.

On October 2, 2008 the District implemented an automatic Email Archiving system. This system captures all emails sent and received via the District Email Server.

It is the District's responsibility to assure the proper archiving of public records is functioning to comply with State statutes and the new FRCP. If you have any questions please contact a member of the Educational Technology Help Desk.

If the personal folders being used to transfer E-mails are located on the workstation, the user is responsible for the periodic backup of these folders.

The following E-mail folders hosted on the mail servers, also known as user mailboxes, are NOT subject to deletion: Calendar, Contacts, Tasks, and Journal.

Revised 5/04
Revised 12/05
Revised 2/15/07
Revised 9/07
Revised 10/08
Revised 7/28/16