SECTION: OPERATIONS

POLICY: 824

TITLE: RECORDS MANAGEMENT

ORIGINAL: May 22, 2017
CURRENT REVISION: April 4, 2022
LAST REVIEWED BY THE COMMTTEE:

ADMINISTRATIVE GUIDELINES

A. Physical Records
    a. Physical records, which include all records not stored electronically, shall be retained and disposed of in accordance with the Records Management Plan.
    b. Physical records shall be indexed in an organized and consistent manner, reflecting the way records will be retained and referenced for later retrieval.
    c. The District shall develop and maintain adequate and up-to-date documentation about each physical record system. Such documentation shall:
        i. List the title of the physical record system and responsible employee(s) or office.
        ii. Define the contents of the system, including formats for record retention.
        iii. Identify vital records and information.
        iv. Determine restrictions on access and use.

B. Electronic Records
    a. Electronic records shall be retained and disposed of in the same manner as records in other formats and in accordance with the Records Management Plan.
    b. Electronic records shall be indexed in an organized and consistent manner, reflecting the way the records will be retained and referenced for later retrieval.
    c. The District shall develop and maintain adequate and up-to-date documentation about each electronic record system. Such documentation shall:
        i. List the title of the physical record system and responsible employee(s) or office.
        ii. Specify all technical characteristics necessary for reading or processing the records stored on the system.
        iii. Identify all defined inputs and outputs of the system.
        iv. Determine the contents of the system, including records formats and database tables.
        v. Identify vital records and information.
        vi. Determine restrictions on access and use.
        vii. Describe update cycles or conditions.

d. The District shall develop and maintain an effective and up-to-date electronic records security program as follows:
    i. Ensure that only authorized personnel have access to electronic records.
    ii. Provide for backup and recovery of electronic records to protect against information loss. The Technology Director shall establish document disaster recovery plans and procedures for electronic records systems. Disaster recovery plans and procedures must be reviewed and updated at least annually.
    iii. Ensure District personnel are trained to safeguard sensitive or classified electronic information.
    iv. Minimize the risk of unauthorized alteration or erasure of electronic records.

C. Email Records
    a. The existence of an email message does not specifically mean that the email constitutes a record. Retention and disposition of email messages depend on the function and content of the email individual message.
    b. Work-related and/or student-related emails and/or emails that document a transaction or activity of the school district are District records and must be treated as such.
    c. Each email user must take responsibility for sorting out personal messages from work-related messages and retaining District records as directed in accordance with Records Retention Schedule and District policies.
    d. Records on an email system, including messages and attachments, shall be retained and disposed of in accordance with the District's Records Management Plan and Records Retention Schedule.
    e. It is the responsibility of the Director of Technology to ensure that all email servers and email archiving devices are properly configured and activated to perform archiving of all emails managed by servers belonging to the District.
    f. All emails shall be archived as required under the District' records retention schedule.
    g. For each E-mail considered a record, the following information shall be retained:
        i. Message content.
        ii. Name of sender.
        iii. Name of recipient.
        iv. Date and time of transmission and/or receipt.
    h. A stand-alone appliance or other suitable solution that combines archive and data compression technology may archive emails. A comprehensive email archive solution is required.
    i. Requirements of the data archive shall be:
        i. Must be able to capture and store all inbound, outbound and internal email.
        ii. User-friendly interface available for search, restore and administrative functions.
        iii. Include full-text and wildcard search functionality on both e-mail body and attachment text.
        iv. Schedulable full and incremental backup capabilities.
        v. Ability to restore easily emails when necessary.
        vi. Emails may be viewed but not altered or deleted during the District's defined retention window.
        vii. Data compression for efficient disk utilization.

viii. Data integrity encryption or assurance that restore data has not been altered in any way.

D. Backup Files

a. The Technology Director and/or Technology Department shall perform backups on a regular schedule of the E-mail and electronic files stored on District servers. These backup are needed for system restoration/or as needed for litigation/investigative purposes

b. The litigation hold directive supersedes the requirements of any records retention schedule that may have otherwise required for the transfer, disposal or destruction of the relevant documents, until the Superintendent has cleared the litigation hold in writing after consultation with the District Solicitor.

c. No employee who has been notified of a litigation hold may alter or delete any physical or electronic record that falls within the scope of that litigation hold.