Use of Email in the School District

Document Information

Last revision date:	April 16, 2018
Adopted date:	
Next review:	January 1 Annually

Overview

Electronic mail or email is a valuable business communication tool, and users shall use this tool in a responsible, effective and lawful manner. Every employee/ authorized user has a responsibility to maintain the District's image and reputation, to be knowledgeable about the inherent risks associated with email usage and to avoid placing the School District at risk. Although email seems to be less formal than other written communication, the same laws and business records requirements apply. School District employees/authorized users shall use the District's designated email system, such as Microsoft Exchange/Outlook, for all business email, including emails in which students or student issues are involved.

Employee Acknowledgement

All employees and authorized users shall acknowledge annually and follow the District's policies and regulations on acceptable use of computerized information resources, including email usage.

Classified and Confidential

District employees and authorized users may not:

a) Provide lists or information about District employees or students to others and/or classified information without approval. Questions regarding usage and requests for such lists or information should be directed to a Principal/supervisor.
b) Forward emails with confidential, sensitive, or secure information without Principal/supervisor authorization. Additional precautions, such as encryption, should be taken when sending documents of a confidential nature.
c) Use file names that may disclose confidential information. Confidential files should be password protected and encrypted. File protection passwords shall not be communicated via email correspondence.
d) Use email to transmit any individual's personal, private and sensitive information (PPSI). PPSI includes social security number, driver's license number or non-driver ID number, account number, credit/debit card number and security code, or any access

code/password that permits access to financial accounts or protected student records without Principal/supervisor authorization.

e) Send or forward email with comments or statements about the District that may negatively impact it.
f) Send or forward email that contains confidential information subject to Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), and other applicable laws without Principal/supervisor authorization.

Personal Use

Employees and authorized users may use the District's email system for limited personal use. However, there is no expectation of privacy in email use. Personal use should not include chain letters, junk mail, and jokes. Employees and authorized users shall not use the District's email programs to conduct job searches, post personal information to bulletin boards, blogs. Chat groups and list services, etc. without specific permission from the Principal/ supervisor. The District's email system shall not be used for personal gain or profit.

Email Accounts

All email accounts on the District's system are the property of the School District.

Receiving Unacceptable Mail

Employees and authorized users who receive offensive, unpleasant, harassing or intimidating messages via email or instant messaging shall inform their Principal/supervisor immediately.

Records Management and Retention

Retention of email messages are covered by the same retention schedules as records in other formats, but are of a similar program function or activity. Email shall be maintained in accordance with the NYS Records Retention and Disposition Schedule ED-1 and as outlined in the Records Management Policy. Email records may consequently be deleted, purged or destroyed after they have been retained for the requisite time period established in the ED-1 schedule.

Archival of Email

All email sent and received to an employee's email account should be archived by the District for a period of no less than six years. This time period was determined based on the possibility of emails that are the official copy of a record according to schedule ED-1. Depending on the District's archival system, employees may have access to view their personal archive, including deleted email.

Training

Employees/authorized users should receive regular training on the following topics:

a) The appropriate use of email with students, parents and other staff to avoid issues of harassment and/or charges of fraternization.
b) Confidentiality of emails.
c) Permanence of email: email is never truly deleted, as the data can reside in many different places and in many different forms.
d) No expectation of privacy: email use on District property is NOT to be construed as private.

Sanctions

The Director of Educational Technology may report inappropriate use of email by an employee/authorized user to the employee/authorized user's Principal/supervisor who will take appropriate disciplinary action. Violations may result in a loss of email use, access to the technology network and/or other disciplinary action. When applicable, law enforcement agencies may be involved.

Notification

All employees/authorized users will be required to access a copy of the District's policies on staff and student use of computerized information resources and the regulations established in connection with those policies. Each user will acknowledge this employee/designated user agreement before establishing an account or continuing in his/her use of email.

Confidentiality Notice

A standard Confidentiality Notice may automatically be added to each email as determined by the District.