ACTIVITIES
6411 USE OF EMAIL IN THE SCHOOL DISTRICT

Overview

Email is a valuable tool that allows for quick and efficient communication. However, careless, unacceptable, or illegal use of email may place the District and members of its community at risk. Use of email in the District must be consistent with the District's educational goals and comply with federal and state laws and regulations, as well as all applicable District policies, regulations, procedures, collective bargaining agreements, and other related documents such as the District's *Code of Conduct*. This includes, but is not limited to, this policy and the District's policies on non-discrimination and anti-harassment, protecting the personal information of District employees and students, acceptable use, and record management.

District-related emails are most secure and best managed when District email services are used. Accordingly, the District's email services should be used for all district-related emails, including emails in which students or student issues are involved. Personal email accounts should not be used to conduct District-related business. Further, District email accounts should not be used as any individual's primary personal email address.

Scope and Application of Policy

This policy applies to all District employees and any individual assigned a District email address to conduct District-related business (authorized user).

Sending Emails with Personal, Private, and Sensitive Information

Personal, private, and sensitive information (PPSI) is any information to which unauthorized access, disclosure, modification, destruction, use, or disruption of access or use could have or cause a severe impact on critical District functions, employees, students, third parties, or other individuals or entities. For purposes of this policy, PPSI includes, but is not limited to:

a) District assessment data;

b) Protected student records;

c) Information subject to laws protecting personal information such as Family Educational Rights and Privacy Act (FERPA), Individuals with Disabilities Act (IDEA), Health Insurance Portability and Accountability Act (HIPAA);

d) Social security numbers;

e) Driver's license or non-driver identification card numbers;

f) Credit or debit card numbers;

g) Account numbers;

h) Passwords; and

i) Access codes.

The failure to follow proper security protocols when emailing PPSI increases the risk that unauthorized individuals could access and misuse PPSI.

District employees and authorized users may not send or forward emails that include:

a) PPSI without building principal or supervisor authorization. Additional precautions, such as encrypting the email in a District-approved method, should be taken when sending any emails containing PPSI.

b) Lists or information about District employees without building principal or supervisor authorization.

c) Attachments with file names that may disclose PPSI. Files containing PPSI should be password protected and encrypted. File protection passwords should not be transmitted via email. District employees and authorized users will not use cloud-based storage services (such as Dropbox or OneDrive) to transmit files with PPSI without previous District approval or consulting with a building principal or supervisor.

d) Comments or statements about the District that may negatively impact it.

Any questions regarding the District's protocols for sending emails with PPSI or what information may or may not be emailed should be directed to a supervisor.

Receiving Suspicious Emails

Social engineering attacks are prevalent in email. In a social engineering attack, an attacker uses human interaction (social skills) to obtain confidential or sensitive information.

Phishing attacks are a form of social engineering. Phishing attacks use fake email messages pretending to represent a legitimate person or entity to request information such as names, passwords, and account numbers. They may also deceive an individual into opening a malicious webpage or downloading a file attachment that leads to malware being installed.

Malware is malicious software that is designed to harm computer systems. Malware may be inadvertently installed after an individual opens an email attachment, downloads content from the Internet, or visits an infected website.

Before responding to any emails, clicking on any hyperlinks, or opening any attachments, District employees and authorized users should review emails for indicators of suspicious activity. These indicators include, but are not limited to:

a) Attachments that were not expected or make no sense in relation to the email message;

b) When the recipient hovers the mouse over a hyperlink that is displayed in the email, the link to the address is for a different website;

c) Hyperlinks with misspellings of known websites;

d) The sender is not someone with whom the recipient ordinarily communicates;

e) The sender's email address is from a suspicious domain;

f) Emails that are unexpected, unusual, or have bad grammar or spelling errors; and

g) Emails asking the recipient to click on a link or open an attachment to avoid a negative consequence or to gain something of value.

District employees and authorized users should forward suspicious emails to the District's information technology (IT) staff.

No Expectation of Privacy

District employees and authorized users should have no expectation of privacy for any email messages they create, receive, or maintain on their District email account. The District has the right to monitor, review, and audit each District employee's and authorized user's District email account.

Accessing District Email Services on Personal Devices

In the event a District employee or authorized user loses a personal device that has been used to access the District's email service, that District employee or authorized user should notify the Districts' IT staff so that measures can be taken to secure the email account.

Personal Use

The District's email services are intended for District-related business only. Incidental or limited personal use of the District's email services is allowed so long as the use does not interfere with job performance. However, District employees and authorized users should have no expectation of privacy in this email use.

The District's email services should not be used to conduct job searches, post personal information to bulletin boards, blogs, chat groups, and list services, etc. without authorization from a building principal or supervisor.

It is prohibited to use the District's email services for:

a) Illegal purposes;

b) Transmitting threatening, obscene, discriminatory, or harassing materials or messages;

c) Personal gain or profit;

d) Promoting religious or political causes; and/or

e) Sending spam, chain letters, or any other type of unauthorized widespread distribution of unsolicited mail.

Personal email accounts or services (Yahoo, Gmail, etc.) should not be accessed via the District Computer System (DCS) without authorization from a building principal or supervisor.

Confidentiality Notice

A standard confidentiality notice will automatically be added to each email as determined by the District.

Training

District employees and authorized users will receive ongoing training related to the use of email in the District. This training may cover topics such as:

a) What is expected of users, including the appropriate use of email with students, parents, and other individuals to avoid issues regarding harassment and/or charges of fraternization;

b) How to identify suspicious emails, as well as what to do after receipt of a suspicious email;

c) Emailing PPSI;

d) How to reduce risk to the District;

e) Cost of policy non-compliance;

f) Permanence of email, including how email is never truly deleted, as the data can reside in many different places and in many different forms; and

g) How users should have no expectation of privacy when using the DCS or any District email service.

Notification

The District will provide annual notification of this policy and any corresponding regulations to all District employees and authorized users. The District will then require that all employees and authorized users acknowledge that they have read, understood, and will comply with the policy and regulations.

Records Management and Retention

The same laws and business records requirements apply to email as to other forms of written communication.

Email will be maintained and archived in accordance with Retention and Disposition Schedule for New York Local Government Records (LGS-1) and as outlined in any records management policies, regulations, and/or procedures.

Additionally, emails may be subject to disclosure under the Freedom of Information Law (FOIL), a court action, an audit, or as otherwise required or permitted by law or regulation.

Disciplinary Measures

Failure to comply with this policy and any corresponding regulations or procedures may subject a District employee and authorized user to discipline such as loss of email use, loss of access to the DCS, and/or other disciplinary action up to and including termination. When applicable, law enforcement agencies may be contacted.

The District's IT staff may report inappropriate use of email by a District employee or authorized user to the District employee or authorized user's building principal or supervisor who may take appropriate action which may include disciplinary measures.

Policy Cross References:
#3320 -- Confidentiality of Computerized Information
#3420 -- Non-Discrimination and Anti-Harassment in the District
#5670 -- Records Management
#6410 -- Staff Acceptable Use Policy
#8271 -- Internet Safety/Internet Content Filtering