Personnel

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES AND EMAIL

The Board of Education will provide staff with access to various computerized information resources through the District Information Systems ("DIS" hereafter) consisting of software, hardware, computer networks, wireless networks/access and electronic communication systems. This access may include, but not be limited to, electronic mail, online services and the Internet. It may also include the opportunity for staff to have independent access to the DIS from their home or other remote locations, and/or to access the DIS from their personal devices. All use of the DIS and the wireless network, including independent use off school premises and use on personal devices, shall be subject to this policy and accompanying regulations.

The Board encourages staff to make use of the DIS to explore educational topics, conduct research and contact others in the educational world. The Board anticipates that staff access to various computerized information resources will both expedite and enhance the performance of tasks associated with their positions and assignments. To that end, the Board directs the Superintendent or his/her designee(s) to provide staff with training in the proper and effective use of the DIS.

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance shall apply to use of the DIS. Employees are expected to communicate in a professional manner consistent with applicable District policies and regulations governing the behavior of school staff.

Access to confidential data is a privilege afforded to District employees in the performance of their duties. Safeguarding this data is a District responsibility that the Board of Education takes very seriously. Consequently, District employment does not automatically guarantee the initial or ongoing ability to use mobile/personal devices to access the DIS and the information it may contain.

This policy does not attempt to articulate all required and/or acceptable uses of the DIS; nor is it the intention of this policy to define all inappropriate usage.

District staff shall also adhere to the laws, policies and rules governing computers including, but not limited to, copyright laws, rights of software publishers, license agreements, and rights of privacy protected by federal and state law.

Staff members who engage in unacceptable use may lose access to the DIS and may be subject to further discipline under the law and in accordance with applicable collective bargaining agreements. Legal action may be initiated against a staff member who willfully, maliciously or unlawfully damages or destroys property of the District.

(continued)

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES AND EMAIL (Cont.)

Social Media Use by Employees

The School District recognizes the value of teacher and professional staff inquiry, investigation and communication using new technology tools to enhance student learning experiences. The School District also realizes its obligations to teach and ensure responsible and safe use of these new technologies. Social media, including social networking sites, have great potential to connect people around the globe and enhance communication. Therefore, the Board of Education encourages the use of District approved social media tools and the exploration of new and emerging technologies to supplement the range of communication and educational services. A school-based social media registry has been established for teachers to obtain District approval before setting up a professional social media presence.

The definition of District approved password-protected social media tools are those that fall within the District's electronic technology network or which the District has approved for educational use. Within these internal forums, the District has greater authority and ability to protect minors from inappropriate content and can limit public access.

The use of social media (whether public or internal) can generally be defined as Official District Use, Professional/Instructional Use and Personal Use. The definitions, uses and responsibilities will be further defined and differentiated in the Administrative Regulation. The School District takes no position on an employee's decision to participate in the use of social media for personal use on personal time. Employees are encouraged to maintain the highest levels of professionalism when communicating in their professional capacity as educators. They have a responsibility to address inappropriate behavior or activity on these networks, including requirements for mandated reporting and compliance with all applicable District Policies and Regulations.

Confidentiality, Private Information and Privacy Rights

Confidential and/or private data, including but not limited to, protected student records, employee personal identifying information, and District assessment data, shall only be loaded, stored or transferred to District-owned devices which have encryption and/or password protection. This restriction, designed to ensure data security, encompasses all computers and devices within the DIS, any mobile devices, including flash or key drives, and any devices that access the DIS from remote locations. Staff will not use email to transmit confidential files in order to work at home or another location. The District has contracted for a secure file share platform (Serv-U) that should be utilized to share confidential information. Staff will only use District approved cloud-based storage services (such as GCSD Google Drive) for confidential files.

Staff will not leave any devices unattended with confidential information visible. All devices are required to be locked down while the staff member steps away from the device, and settings enabled to freeze and lock after a set period of inactivity.

(continued)

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES AND EMAIL (Cont.)

Staff data files and electronic storage areas shall remain District property, subject to District control and inspection. The Technology Coordinator may access all such files and communications without prior notice to ensure system integrity and that users are complying with requirements of this policy and accompanying regulations. Staff should **NOT** expect that information stored on the DIS will be private.

Use of Email in the School District

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 the definition of PII (personally identifiable information as referenced in our Data Security and Privacy Policy). Some examples of PPSI include:

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);

(continued)

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES AND EMAIL (Cont.)

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. The District approved file share platform (Serv-U) should be utilized when there is a need to send PPSI.

b) Lists or information about District employees. The District approved file share platform (Serv-U) should be utilized when there is a need to send PPSI about District employees.

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 only use District approved cloud-based storage services (GCSD Google Drive) or the District approved file share platform (Serv-U) to transmit files with PPSI.

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 or the District's Data Privacy Officer.

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.

(continued)

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES AND EMAIL (Cont.)

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 immediately notify the District Data Privacy Officer or the District's information technology (IT) staff of any suspicious emails.

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.

(continued)

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES AND EMAIL (Cont.)

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

As part of the requirements of State Education Law 2-d, 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.

(continued)

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES AND EMAIL (Cont.)

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.

NOTE: Refer also to Policies #3420 -- Non-Discrimination and Anti-Harassment in the School District
#5670 -- Records Management
#5676 -- Data Security and Privacy
#8271 -- Internet Safety/Internet Content Filtering Policy
#5672 -- Information Security Breach and Notification

Adoption Date: 8/5/96
Revised: 7/6/98; 8/26/13; 11/18/13; 11/04/19; 3/29/21; 9/9/24