Human Resources

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES

I. DISTRICT COMPUTER SYSTEM

The Board of Education will provide staff with access to various computerized information resources through the District's computer system (DCS hereafter) consisting of software, hardware, computer networks, wireless networks/access and electronic communication systems. This may include access to electronic mail, and the Internet. It may also include the opportunity for staff to have independent access to the DCS from their home or other remote locations, and/or to access the DCS from district-owned or their personal devices. All use of the DCS and the wireless network, including independent use off school premises and use on personal devices, shall be subject to this policy and accompanying regulations. Every employee/authorized user has a responsibility to maintain the District's image and reputation, to be knowledgeable about the inherent risks associated with social media and email usage and to avoid placing the School District at risk.

The Board encourages staff to make use of the DCS 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. Toward that end, the District should provide staff with notification in the proper and effective use of DCS.

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.

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance shall apply to use of the DCS. 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 may be required of District employees in the performance of their duties. Safeguarding this data is a District obligation that the Board of Education takes very seriously. Employees have a responsibility to maintain confidentiality when utilizing electronic mail and/or when accessing the DCS on or off school grounds. District employment does not automatically guarantee the initial or ongoing access the DCS and the information it may contain.

This policy does not attempt to articulate all required and/or acceptable uses of the DCS; nor is it the intention of this policy to define all inappropriate usage. The Superintendent will further define general guidelines of appropriate staff conduct and use as well as proscribed behavior. The staff will be notified.

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

Staff members who engage in unacceptable use may lose access to DCS 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

II. SOCIAL MEDIA USE BY EMPLOYEES

The School District recognizes the value of teacher and professional staff inquiry, innovation, 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. 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 and social media site usage and to avoid placing the School District at risk.

For purposes of this Policy, the definition of public social media networks or Social Networking Sites (SNS) are defined to include: websites, applications, Web logs (blogs), wikis, social networks, online forums, virtual worlds, video sites and any other social media generally available to the School District Community which do not fall within the District's electronic technology network. 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. Employees have the right to decide whether or not to participate in the use of social media or SNS for personal use on personal time. Employees should maintain the highest level of professionalism, when communicating on social media or SNS, whether using District devices or their own personal devices, as the District views employees as role models both at school and away from school. Communications which disrupt co-worker relations, erodes a close working relationship premised on professionalism and confidentiality, and/or interferes with the performance of an employee's duties may be deemed inappropriate. Employees 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.

Commented [T1]: Generally, you would have the right to restrict personal activities while using district devices. If you have not done that in the past, then a change would be construed as something that would have to be bargained regarding affiliated staff.

III. USE OF EMAIL IN THE SCHOOL DISTRICT

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, for all business emails, including emails in which student or student issues are involved. All email accounts in the district's system are the property of the school district.

A) 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:

B) Classified and Confidential

District employees and authorized users shall not:

(a) Provide lists or information to external users about District employees or students to others and/or classified information without approval. Questions regarding usage should be directed to a Principal/Supervisor.

(b) Forward emails to external users with confidential, sensitive, or secure information without approval or Administrator/Supervisor authorization. Additional precautions should be taken when sending documents of a confidential nature.

(c) Use file names that may disclose confidential information.

(d) Send or forward email with comments or statements about the District that may negatively impact it.

C) 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. The District has the right to review all employees' email. If employees decide to use the District's email system for personal use, the employee will be held accountable for the content of all incoming and outgoing personal messages. The District has the right to monitor all school district owned email accounts. If the use of an account by an employee is found to be in violation of Federal or State law or regulation, and/or school district policy, and contractual and/or assigned responsibilities, the employee may be subject to prosecution and/or disciplinary action. Employees should maintain the highest level of professionalism, when communicating via email, as the District views employees as role models both at school and away from school. Communications which disrupt and/or interferes with the performance of any employee's duties may be deemed inappropriate.

D) Email Accounts

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

E) Receiving Unacceptable Emails

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

F) Records Management and Retention

Retention of email messages are covered by the same retention schedules as records in other formats, but are for 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.

G) 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 (6) years. This time period was determined based on the possibility of emails that are the official copy of a record according to school schedule ED-1. Depending on the District's archival system, employees may have access to view their personal archive, including deleted email.

H) Employee Notice

Employees will be informed of the District Policy at the time of hire. Employees/authorized users should receive regular notification 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, including email response expectations

(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

I) Sanctions

District staff should 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 loss of email use, access to technology network and/or disciplinary action. When applicable, law enforcement agencies may be involved.

J) 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.

K) Confidentiality Notice

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

L) Confidentiality, Privacy 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 DCS, any mobile devices, including flash or key drives, and any devices that access the DCS from remote locations. Staff will not use email to transmit confidential files in order to work at home or another location or cloud based storage services (such as Dropbox, Google drive, SkyDrive, etc.) for confidential files.

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

Staff data files and electronic storage areas shall remain District property, subject to District control and inspection. The Superintendent and/or his designee 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 DCS will be private.

First Reading: April 21, 2016
Second Reading: May 5, 2016
Adoption: May 26, 2016