SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES

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, so-called "on-line services" 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 their personal devices. All use of the DCS and the wireless network, including independent use of school premises and use on personal devices, shall be subject to this policy and accompanying regulations.

The Board encourages staff to makes 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. 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 DCS.

Staff use of the DCS is conditioned upon written agreement by the staff member that use of the DCS will conform to the requirements of this policy and any regulations adopted to ensure acceptable use of the DCS. All such agreements shall be kept on file in the District Office.

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. Electronic mail and telecommunications are not to be utilized to share confidential information about students or other employees.

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 seriously. Consequently, District employment does not automatically guarantee the initial or ongoing ability to use mobile/personal devices to 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. Administrative regulations will further define general guidelines of appropriate staff conduct and use as well as proscribed behavior.

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 the rights and privacy protected by federal and state law.

Staff members who engage in unacceptable use may lose access to the 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.

(Continued)

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES

Personal Use of Social Media by Employees

It is the responsibility of all District employees to protect and further the District's values and mission. This includes all dealings with students, employees, parents, and the public. The creation and expansion of social media, social networking, personal/business websites, blogs, and other virtual or online media, which will collectively be referred to as social networking sites or "SNS", have dramatically expanded the opportunities for communication by and with District employees. Therefore, the District has developed these standards for employee behavior in or on SNS.

The District's expectations for employees who choose to use SNS for personal reasons (*i.e.*, use of SNS that is not related to an employee's job duties for the District) are as follows:

1. The District prohibits personal use of SNS during work hours and on District-owned hardware.
2. If a District employee's SNS profile identifies or references the District in any way, or if the District could be connected to the account, it is the employee's responsibility to ensure that his/her comments and all content posted are appropriate, respectful, and professional. Please keep in mind that many District employees are well-known in their communities and any posting may be viewed as connected to the District.
3. Online behavior should reflect the same standards of honesty, respect, and consideration that are used in face-to-face contact. An employee's online communication could be interpreted as an extension of the employee's office or classroom. What is inappropriate in the office or classroom is also inappropriate online. Any post, comment or communication related to the District should always meet the highest standards of professional discretion and shall comply with all applicable District policies and regulations.
4. District employees may not use SNS as a mechanism to harass or otherwise harm other District employees, students or community members, or make comments or statements or take any action in any online forum which discriminates against, attacks, threatens, or otherwise harms any other District employee, student, or community member.
5. If posting comments or viewpoints on topics related to the District, District employees should state that the information is representative of the employee's views and opinions and not necessarily the views and opinions of the District. District employees should not state or give the impression that they are speaking on behalf of the District.
6. District employees may not disclose confidential information, including any information about a student, project, or personnel matter/issue.
7. District employees must comply with applicable laws regarding the use and disclosure of copyrighted materials.

(Continued)

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES

8. District personnel are prohibited from using SNS to create or maintain personal relationships with students. For purposes of these guidelines, "personal relationships with students" means any behavior or conduct that is unrelated to course work or official school matters. Such behavior may erode the professional authority and traditional roles of teacher and student within the District and may violate District policies and/or regulations.

   Employees may not “friend”, “follow”, direct message, or otherwise connect with current students or any student currently enrolled in any school within the District Pre-K through 12, nor should they accept a “friend”, “follow” or other similar request if prompted by a current District student. Be mindful that many former students have online connections with current students. Information shared between District staff and former students is likely to be seen by current students as well.

   If your position within the District requires communication with students or parents that is related to course work or official school matters, the District network, email, teacher web pages within the District website, and school-provided/owned equipment must be used when communicating online.

9. District employees should not post or allow others to post to their SNS statements or images that could be deemed harmful to the District’s reputation or in violation of District policies or the law.

10. District employees may not make disparaging or inappropriate comments or statements about the District that do not align with the goals and mission of the District that are not protected under the First Amendment to the United States Constitution and/or applicable labor law.

11. The District recognizes that employees are entitled to free speech protections under the First Amendment to the United States Constitution when they speak as a private citizen on a matter of public concern. However, a District employee may be subject to discipline or discharge if his/her speech causes disruption to the District’s operations or threatens to interfere with such operations.

12. An employee’s communications online may be seen by others as a reflection or representation of the employee’s character, judgment, and values, and in some instances may be perceived by others as an indirect extension of the District, regardless of the employee’s intent. Posting some types of information may jeopardize the employee’s image and reputation and, by extension, the District’s image and reputation.

(Continued)

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES

13. Be mindful that even the most stringent privacy settings do not guarantee that a District employee's communications will not be seen or shared. Information shared online may be posted in perpetuity, may be impossible to retrieve or delete, and may be forwarded or endlessly shared. District employees should assume and conduct themselves as if everything they post online will be made public.

14. District employees will promptly cooperate with District administration in removing any Internet data or postings that violate this policy.

Reporting Violations

Do not underestimate the power and speed of SNS. Irreparable damage can result from certain postings in a very short time, so it may be imperative that the District take immediate action with respect to violations of this policy. The District will investigate inappropriate usage and will respond to complaints made about posting/sites in violation of District policies.

If any District employee becomes aware of any online posting that is in violation of this policy or other District policies, the District employee must share that information with their Principal, direct supervisor or the Superintendent. Failure to report known abuse may constitute grounds for discipline in accordance with legal guidelines, District policy and regulations, and the applicable collective bargaining agreement.

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 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. Staff will not use cloud-based storage services (such as Dropbox, Google Drive, SkyDrive, etc.) 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.

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

(Continued)

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES

NOTE: Refer also to Policies # 5672--Information Security Breach and Notification
6411—Staff Use of Email
7243—Student Data Breaches
7316—Student Use of Personal Technology
8271—Internet Safety/Internet Content Filtering Policy

Adoption Date 10/20/20