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. All use of the DCS, including independent use off school premises, shall be subject to this policy and accompanying regulations.

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 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 electronic confirmation by the staff member that use of the DCS will conform to the requirements of this policy and any regulations adopted to insure acceptable use of the DCS.

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 very 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. (Refer to Policy 5830: Personally Owned Computer Support)

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 rights of 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 (CONT'D.)

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, GoogleDrive, 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 are and shall remain District property, subject to District control and inspection. The Superintendent or the Superintendent's designee may access all such files and communications at any time and without prior notice to insure system integrity and that users are complying with requirements of this policy, related policies, and accompanying regulations. Staff should **NOT** expect that information sent, received, created, modified or stored on the DCS will be private, **as persons using the DCS have no right of privacy in such use**.

Intellectual Property

Any product, document, e-mail, etc. created on the District Computer System, or an individual's computer system for a work-related purpose(s), is and shall remain the exclusive property of the District.

Implementation

Administrative regulations will be developed to implement the terms of this policy, addressing general parameters of acceptable staff conduct as well as prohibited activities so as to provide appropriate guidelines for employee use of the DCS.

NOTE: Refer also to Policy #5840 - Email Use in the School
Policy #8271 -- Children's Internet Protection Act: Internet Content Filter/Safety
Policy #7314 -- Student Use of Computerized Information Resources
Policy #5841 – Use of Social Media, Web Tools & Teacher Web Pages

Adopted: 7/10/2001
Revised: 1/09/2007, 2/14/2012, 8/26/2014
Reviewed by Superintendent and Director of Information Technology on 5/18/2020 with no recommended changes; approved by BOE 5/26/2020