SUBJECT: STAFF ACCEPTABLE USE POLICY

The Board will provide staff with access to various computerized information resources through the District's computer system (DCS) consisting of software, hardware, computer networks, wireless networks/access, and electronic communication systems. This may include access to electronic mail, 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 off school premises and use on personal devices, will be subject to this policy and any 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. To that end, the Board directs the Superintendent or 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 all policies and any regulations adopted to ensure acceptable use of the DCS.

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance will 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 will not 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 takes very seriously. Consequently, District employment does not automatically guarantee the initial or ongoing ability to use mobile or 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 will 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 ACCEPTABLE USE POLICY (Cont'd.)

Confidentiality, Private Information and Privacy Rights

Confidential or private data, including, but not limited to, protected student records, employee personal identifying information, and District assessment data, will 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. Similarly, staff are prohibited from using private cloud-based storage services (such as Dropbox, GoogleDrive, SkyDrive, etc.) for confidential files.

In addition, staff will not leave any devices unattended with confidential information visible. All devices must 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 will remain District property, subject to District control and inspection. Upon approval by the Superintendent, the Chief Information Officer or designee may access all staff data files and communications without prior notice to ensure system integrity and that users are complying with requirements of this policy and any accompanying regulations.

Staff should NOT expect that their use of and/or information stored on the DCS will be private. At the end of employment and/or upon the District's request, staff members will return any computer, equipment, mobile device, and/or accessories they have been assigned.

NOTE: Refer also to Policies #5672 -- Information Security Breach and Notification
#5674 -- Data Networks and Security Access
#6411 -- Use of Email in the District
#7316 -- Student Use of Personal Technology
#8271 -- Internet Safety/Internet Content Filtering Policy

Adopted: 6/22/99
Revised: 9/6/22