

Personnel

SUBJECT: STAFF ACCEPTABLE USE POLICY (AUP)

The Board will provide staff with access to various computerized information resources through the District's computer system (DCS hereafter) consisting of software, hardware, computer networks 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 some 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 or her designee(s) to provide staff with training in the proper and effective use of the DCS.

Staff use of the DCS is required to perform job duties, it is expected that use of the DCS will conform to the requirements of this policy 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 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 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.

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 ACCEPTABLE USE (Cont'd.)**Social Media Use by Employees**

The District recognizes the value of teacher and professional staff inquiry, investigation and communication using new technology tools to enhance student learning experiences. The 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 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.

For purposes of this Policy, the definition of **public social media networks or Social Networking Sites (SNS)** are defined to include: websites, Web logs (blogs), wikis, social networks, online forums, virtual worlds, and any other social media generally available to the District community which do not fall within the District's electronic technology network (e.g., Facebook, MySpace, Twitter, LinkedIn, Flickr, Vine, Instagram, blog sites, etc.). 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 District takes no position on an employee's decision to participate in the use of social media or SNS for personal use on personal time. However, personal use of these media during District time or on District-owned equipment is *allowed* for educational purposes on a limited basis. In addition, employees are encouraged to maintain the highest levels of professionalism. They have responsibility for addressing 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 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.

(Continued)

SUBJECT: STAFF ACCEPTABLE USE POLICY (AUP) (Cont'd.)

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 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 DCS will be private.

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 Policies #5614 -- Email Communications and Archival
#5682 -- Information Security Breach and Notification
#8264 -- Internet Safety/Internet Content Filtering Policy
#8265 -- Student Use of Personal Technology

Adopted: 12/17/98

Revised: 7/1/08; 7/10/12; 11/5/13; 5/9/17