| | |
|---|---|
| Book | Policy |
| Section | 6000 Personnel |
| Title | Staff Use of Computerized Information Resources |
| Code | 6410 |
| Status | Active |
| Adopted | December 15, 2003 |
| Last Revised | January 11, 2016 |
| Prior Revised Dates | 9/18/06 |

**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, Cloud 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, including independent use off school premises and use on personal devices, 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 collaborate or communicate with others in support of the district mission. 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 district shall provide ongoing professional development to afford staff the requisite skills and best practices to promote the use of the DCS in a secure and efficacious manner.

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.

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. As such, the district expects all staff to adhere to any and all guidelines and best practices provided, especially as it relates to confidential or other personal, private, sensitive information (PPSI). 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.

**Social Media Use by Employees**

The School District recognizes the value of teacher and professional staff inquiry, 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. Therefore, the Board of Education 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, 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. The School 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 discouraged. In addition, employees are encouraged to maintain the highest levels of professionalism when communicating, whether using District devices or their own personal devices, in their professional capacity as educators. They 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.

**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 outside of the district network in order to work at home or another location. Staff will not use cloud-based storage services (such as Dropbox, GoogleDrive, SkyDrive, etc.) for PPSI 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 personal/mobile devices must be set to freeze and lock after a set period of inactivity.

Staff data files and network/cloud storage shall remain District property, subject to District control and inspection. The Senior Technical Specialist 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.

**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 #5672 -- Information Security Breach and Notification
#5674 -- Data Networks and Security Access
#5676 -- Privacy and Security for Student Data and Teacher and Principal Data
#6411 -- Use of Email in the District
#7315 -- Student Use of Personal Technology
#8271 -- Internet Safety/Internet Content Filtering Policy

Adopted: 12/15/03
Revised: 9/18/06; 1/11/16