| Doc Library<br>Main Topic<br><br>Jacquelyn Wopperer<br>11/08/2017 11:34 AM | **Subject:** **# 6430 Staff Acceptable Use Policy**<br><br>**Category:** 6400 Series – Personnel Activities |
|---|---|

# PERSONNEL ACTIVITIES
## Staff Acceptable Use Policy

The Board shall 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 personal devices. All use of the DCS and the wireless network, including use of personal devices, will be subject to this policy.

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 this policy and any regulations adopted to ensure acceptable use of the DCS. These agreements will be kept on file in the District Office.

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, employees or other district matters.

Access to confidential data is a privilege afforded to District staff 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 the District Computer System ("DCS") and the information contained therein.

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.

District staff will also adhere to the laws, policies, and rules governing computers/technology usage 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 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 (SNS), 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.

Public social media networks or 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 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 or Personal Use. Personal use of social media or SNS by employees during District time or on District-owned equipment is prohibited. 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 or private data, including, but not limited to, protected student records, employee personal identifying information (PII), 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 addition, staff will not leave any devices unattended. 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. The Technology Coordinator 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 information stored on the DCS will be private.

**Staff Use of Personal Technology**
All staff who use mobile technology in the course of their job duties, must comply with this policy which governs the use of this type of equipment when it is used in conjunction with the District's wireless network or in the course of the staff member's job duties.

Access to confidential data is a privilege afforded to District staff 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 personal devices to access the District Computer System ("DCS") and the information contained therein.

**Personally Owned Devices**

Staff may choose to use their own personal devices to perform job-related functions, rather than the technology assigned to them by the district. If a staff member chooses to use his or her own personal technology equipment, the following guidelines will apply:

1. Personal devices connected to the DCS/District wireless network must have updated and secure operating systems and have their use segregated from District network resources. Staff must notify Technology staff of their planned use of such a device so proper safeguards can be instituted.
2. The entire cost to acquire all personal technology equipment is the responsibility of the staff member. Services that may incur a financial cost to the District, such as phone options or other "apps" are not allowed.
3. Personal technology equipment is not covered by the District's insurance if it is lost, stolen or damaged. Loss or damage to any personal technology equipment is solely the responsibility of the staff member. If lost or stolen, the loss should be reported immediately to Technology staff so appropriate action can be taken to minimize any possible risk to the DCS and the District.
4. Staff assumes complete responsibility for the maintenance of personal devices, including maintenance to conform to District standards. Staff also assumes all responsibility for problem resolution, as well as the use and maintenance of functional, up-to-date anti-virus and ant-malware software and any other protections deemed necessary by Technology staff.
5. Staff must also meet any expectations of continuity in formatting of files, etc. when making changes to document for work purposes (i.e., do not change the format of a file so that the original file is unusable on district-owned hardware or software).
6. All personal technology equipment used on the DCS/District wireless network is subject to review by the District Technology Coordinator, or individuals or entities designated by the Superintendent, if there is reason to suspect that the personal device is causing a problem to the DCS network, or if the staff member is suspected by a supervisor of spending excessive time at work on non-work related matters.
7. The use of personal technology equipment in the course of a staff member's professional responsibilities may result in the equipment and/or certain data maintained on it being subject to review, production and/or disclosure (i.e., in response to a FOIL request, discovery demand or subpoena). The staff is required to submit any such information or equipment, when requested.
8. It is also the responsibility of District staff using a mobile device, personal or District-owned, to ensure that all security protocols normally used in the management of district data on conventional storage infrastructure are also applied on the mobile device. All District-defined processes for storing, accessing, and backing up data must be used on any device used to access the DCS.
9. Staff may access the DCS remotely if the staff member has demonstrated that his or her personal device meets the security standards set by the District.
10. Use of any mobile technology device during the school day, whether District-issued or personally owned, should not interfere with the staff member's ability to carry out daily responsibilities.
11. Software licensed by the school district is not eligible to be installed upon any personally owned devices.
12. District owned peripheral devices (i.e., Smart Boards, Projectors, printers among others) will not be accessible to any personally owned devices.
13. When utilizing any technology devices (personally owned or district asset) staff will adhere to the laws, policies and rules governing computer usage including, but not limited to copyrights, the rights of software publishers, license agreements and the rights of privacy protected by Federal and State law.

**Wireless Devices on District Premises**

1. For security reasons, staff who use their personal device to connect to the Internet, using a district network, will only be permitted to use the District's wireless network. Access to any other District network using a personal device is prohibited.
2. Personal devices that have the ability to offer wireless access to other devices must not be used to provide that functionality to others in or on any District property. Any violation of this condition will result in personal device access privileges being withdrawn.
3. When personal devices are used in district facilities via the District wireless network, the District reserves the right to:
    a. Make determinations on whether specific uses of the personally owned wireless devices are consistent with the Staff Acceptable Use of Technology agreement;
    b. Log network use and monitor storage disk space utilized by such users; and
    c. Remove or restrict the user's access to the network and suspend the right to use the personally owned computer in District facilities at any time if it is determined that the user is engaged in unauthorized activity, violating the District's Staff Acceptable Use of Technology agreement, or violating the terms of this policy.

**Policy Cross References:**

Ref: Policies #5674 Data Networks and Security Access
#5675 Information Security Breach and Notification
#7316 Student Use of Personal Technology
#8342 Internet Safety/Internet Content Filtering

Adoption Date: 7/12/2001, Revised: 9/11/2003, Revised: 7/6/2010, Revised: 11/08/2017