



Book	SW BOCES Policies
Section	6000 - PERSONNEL
Title	STAFF ACCEPTABLE USE POLICY
Code	6413
Status	Active
Adopted	January 17, 2024

The Board of Education will provide staff with access to various computerized information resources through the Southern Westchester BOCES Computer Network (BCN) consisting of software, hardware, devices, computer networks, wireless networks/access, and electronic communication systems. This may include access to email, online services, and the internet. It may also include the opportunity for staff to have access to the BCN from their home or other remote locations, and/or to access the BCN from their personal devices, such as smart phones. All use of the BCN and the wireless network, including use of Southern Westchester BOCES property and use on personal devices, shall be subject to this policy and accompanying regulations.

The Board encourages staff to make use of the BCN to explore educational topics, conduct research and contact others in the educational world. The Board believes that staff access to various computerized information resources will allow staff members to perform their duties better, more quickly and more efficiently. As such, the Board directs the District Superintendent or their designee(s) to provide staff with training in the proper and effective use of the BCN.

Staff are not guaranteed access to the BCN. Staff use of and access to the BCN is conditioned upon compliance with the requirements of this policy and any regulations adopted to ensure acceptable use of the BCN. Staff will be required to acknowledge they have read and understand this policy and any accompanying regulations and that their access and use of the BCN is conditioned on their compliance with this policy and any accompanying regulations.

The same standards of acceptable staff conduct which apply to an employee's job performance also apply to use of the BCN. Employees are expected to communicate in a professional manner, consistent with applicable SWBOCES policies and regulations governing the behavior of staff. Email and/or telecommunications are not to be utilized to share confidential information about students or other employees except as authorized by this policy and accompanying regulation.

Staff personal use of the BCN should be kept to a minimum, may not interfere with the performance of the employee's duties and responsibilities, and should only occur during nonstudent contact times and/or during approved break times. The use of streaming services (personal or work related) such as Hulu, Netflix, Amazon Prime, Amazon Music, Pandora, as well as other streaming services not identified here are not permitted. Questions or concerns regarding the use of these services on the BCN should be directed to the office of the Director of Technology.

This policy does not identify all required and/or acceptable uses of the BCN; nor is it the intention of this policy to define all inappropriate usage. Administrative regulations will further define guidelines of appropriate staff conduct and use as well as prohibited behavior.

SWBOCES staff shall also adhere to the laws, policies and rules that apply to computers and electronic information 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 BCN and may be subject to further discipline under the law and in accordance with any applicable collective bargaining agreements. Legal action may be initiated against a staff member who willfully, maliciously, or unlawfully damages or destroys the property of SWBOCES or its networks.

Social Media Use by Employees

SWBOCES recognizes the value of the use of new technologies to enhance student learning experiences. SWBOCES 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 SWBOCES-approved social media tools and the use of new and emerging technologies to supplement the range of communication and educational services in the employee's role. The definition of SWBOCES-approved password-protected social media tools are those that are part of the SWBOCES electronic technology network and/or those public social media networks or social networking sites (SNS) which the SWBOCES has approved for educational use, where the SWBOCES has greater authority and ability to protect minors from inappropriate content and can limit public access. For purposes of this policy, public social media networks or social networking sites (SNS) are defined to include, but are not limited to: websites, blogs, wikis, social networks, online forums, virtual worlds, video sites and any other social media generally available to the public, including the SWBOCES community (e.g., Pinterest, Facebook, Twitter, LinkedIn, Flickr, Vine, Instagram, SnapChat, blog sites, etc.), which do not fall within the SWBOCES electronic technology network.

Generally, SWBOCES takes no position on an employee's use of social media or SNS on their personal time. However, employees may be subject to discipline for inappropriate personal use of social media or SNS during their personal time where there is a nexus (i.e., connection) between such use and their position in SWBOCES. Personal use of these media during SWBOCES time or on SWBOCES-owned equipment should be kept to a minimum, may not interfere with the performance of the employee's duties and responsibilities, and may only occur during non-student contact times and/or during approved break times. In addition, employees are expected to maintain the highest levels of professionalism when communicating in their professional capacity, whether using SWBOCES devices or their own personal devices. Employees also have a responsibility to address inappropriate behavior or activity on these networks, including requirements for mandated reporting and compliance with all applicable SWBOCES policies and regulations. For more information, please refer to the SWBOCES Social Media Regulation.

Confidentiality, Private Information, and Privacy Rights

Confidential and/or private data, including but not limited to, protected student records, employee personally identifiable information, and assessment data, shall only be loaded, stored, or transferred to SWBOCES-owned devices which have encryption and/or password protection. This restriction, designed to ensure data security, encompasses all computers and devices within the BCN, any mobile devices, including flash or key drives, and any devices that access the BCN from remote locations, such as an employee's home. Staff may not use email to transmit confidential files to themselves or others, to work at home, or another location. Staff may not use personal email accounts to conduct SWBOCES business. Staff may not use personal cloud-based storage services (such as Dropbox, GoogleDrive, One Drive, etc.) for confidential files. Staff are responsible for complying with the requirements of the Family Educational Rights and Privacy Act, New York State Education Law Section 2-d, and Part 121 of the Commissioner's Regulations when storing, accessing, and transmitting confidential student information and data over the BCN.

Staff may not leave any SWBOCES 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 SWBOCES property, subject to SWBOCES control and inspection. SWBOCES may access and/or monitor all such files and communications without prior notice for any reason. Staff should not expect that information stored on the BCN will be private. Staff have no expectation of privacy in any files and/or information contained on the BCN, including but not limited to, any SWBOCES-owned devices/equipment, computers, smart/mobile phones and/or tablets, the SWBOCES network/server and/or the SWBOCES email system.

Rules of Conduct and Compliance

Employees who violate this policy and/or its accompanying regulations may have their access rights suspended or revoked by SWBOCES. In addition, disciplinary action may be taken as permitted by applicable law and the terms of any applicable collective bargaining agreements. A non-exhaustive list of examples of prohibited uses of the BCN is provided in Regulation 6413R.

Implementation

Administrative regulations will be developed to implement the terms of this policy, addressing parameters of acceptable staff conduct as well as prohibited activities to provide appropriate guidelines for employee use of the BCN. This policy is subject to change. SWBOCES reserves the right to restrict or terminate BCN access at any time for any reason. SWBOCES further reserves the right to monitor network activity as it sees fit to maintain the integrity of the BCN and to monitor acceptable use.

Disciplinary penalties will be determined in accordance with applicable law and the terms of applicable collective bargaining agreements. However, revocation of access will be determined by the network administrator, acting in consultation with building and BOCES-wide administrators.

Staff must sign off on an acknowledgment that they have read, understand, and agree to this policy and its accompanying regulation as a condition of use of and access to the BCN.