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

The Southern Westchester BOCES Computer Network (BCN) is provided for staff to enhance the educational programs of SWBOCES, to further SWBOCES goals and objectives, to conduct research, and communicate with others. Staff data files, email and electronic storage areas shall remain SWBOCES property, subject to SWBOCES control and inspection. The Director of Technology may access all such files and communications without prior notice. Staff should not expect that information stored on the BCN will be private, as there is no expectation of privacy in such information or in the BCN.

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance shall apply to staff members' use of the BCN. The standards of acceptable use as well as prohibited conduct by staff accessing the BCN, as outlined in BOCES policy 6413 and this regulation, are not intended to be all-inclusive. Staff members are encouraged to utilize electronic communications in their roles as employees of SWBOCES. Staff are also encouraged to utilize electronic means, such as email, to communicate with parents, legal guardians, o homebound students, subject to appropriate consideration for student privacy. Such electronic communications shall be limited to school related issues or activities. Communications over the BCN are often public in nature; therefore, general rules and standards for professional behavior and communication will apply.

The SWBOCES's policies and accompanying regulations on staff and student acceptable use of computerized information resources establishes guidelines for staff to follow in instruction, working with students, non-instructional capacities, and acceptable student use of the BCN, including access to external computer networks.

Prohibitions

The examples provided are not meant to be an exhaustive list defining all inappropriate use of the BCN. The staff member who commits an act of misconduct which is not specifically addressed in BOCES policy 6413 and/or this regulation may also be subject to disciplinary action in accordance with law and/or the applicable collective bargaining agreement, as well as loss of access to the BCN. Legal action may also be initiated against a staff member who willfully, maliciously, or unlawfully damages or destroys technology-related property of SWBOCES or its networks. In addition to the general requirements of acceptable staff behavior, activities which shall be prohibited by staff members using the BCN include, but are not limited to, the following:

1) Using the BCN which in any way results in unauthorized charges or expense to SWBOCES.

2) Damaging, disabling or otherwise interfering with the operation of computers, computer systems, software, or related equipment through physical action or by electronic means. This includes using the BCN to damage, disable or otherwise interfere with the computers and/or computer systems of any other person or organization.

3) Maliciously accessing, altering, deleting, damaging, or destroying any computer system, computer network, computer program, or data. Such SWBOCES users may be subject to criminal prosecution as well as disciplinary action by SWBOCES. This includes, but is not limited to, changing, or deleting another user's account,
changing the password of another user, using an unauthorized account, damaging any files, altering the system, using the system to make money illegally, destroying, modifying, vandalizing, defacing or abusing hardware, software, technology-related furniture, or any SWBOCES property.

4) Engaging in the modification of any existing software or application on any BCN device, without the express permission of the Director of Technology or their
designee. Any software or applications that are installed must be properly licensed from the software or application copyright owner, and any modifications to
software or applications must comply with the terms of the applicable license(s) and meet all NYSED Data privacy compliance requirements, including, but not limited
to, those required by New York State Education Law Section 2-d, Part 121 of the Commissioner’s Regulations.

5) Changing, copying, renaming, deleting, reading, adding to, or otherwise accessing files or software, with malicious intent, on the BCN and not created by the staff
member doing so without express permission from the Director of Technology.

6) Employing the BCN for commercial purposes, product advertisement, or political lobbying.

7) Engaging in any fundraising without authorization.

8) Disclosing an individual password to others or using others' passwords.

9) Sending or displaying offensive messages or pictures.

10) Using vulgar, derogatory, or obscene language.

11) Harassing, insulting, bullying, threatening, or attacking others.

12) Making or transmitting false, defamatory, or libelous statements about another person, group, or organization.

13) Willfully, maliciously, and/or unlawfully engaging in practices that threaten the BCN (e.g., loading files that may introduce a virus).

14) Violating regulations prescribed by the network provider.

15) Assisting a student, staff member, or any other person in violating SWBOCES policy and/or regulation or failing to report knowledge of any violations of SWBOCES policy and/or regulation on student and/or staff use of computerized information resources.

16) Using the BCN in a manner that violates any other aspect of Board Policy 6413, its regulations, as well as local, state, or federal laws or regulations.

17) Using or installing any unapproved software. All software requests (local installations, web based, or mobile apps) must be submitted to a supervisor for
review and are subject to an established approval process that also includes the SWBOCES Director of Technology and SWBOCES Data Protection Officer. No
unapproved software (locally installed or web based) may be used without review to ensure all aspects of data privacy are upheld, as per NYSED Law, including, but
not limited to, New York State Education Law Section 2-d and Part 121 of the Commissioner’s Regulations.

18) Using personal audio/video streaming services (including but not limited to Pandora, Hulu, Netflix, Amazon Prime, etc.).

19) Using personal movie media (including but not limited to DVDs, Blu-Ray, etc.) for showings that do not meet “fair use” provisions of the United States Copyright Act of 1976. “Fair use" in this context means that the

copyrighted materials of others may be used only for scholarly purposes and that the use must be limited to brief
excerpts. Members of the School Library System can assist employees with fair use
issues.

20) Failing to comply with the "fair use" provisions of the United States Copyright Act of 1976. "Fair use" in this context means that the copyrighted materials of others
may be used only for scholarly purposes and that the use must be limited to brief excerpts. Members of the School Library System can assist employees with fair use
issues.

21) Copying any copyrighted or licensed software from the Internet, from the BCN or from another user without the express permission of the copyright holder. Software must be purchased or licensed before it can legally be used on any SWBOCES owned device in conjunction with but not limited to, New York State Education Law Section 2-d and Part 121 of the Commissioner's Regulations.

22) Violating copyright law, including illegal file sharing, including but not limited to, music, videos, and software.

23) Logging on to someone else's account, attempting to access another user's files, or permitting anyone else to log on to their own accounts. Users may not try to gain unauthorized access ("hacking") to the files or computer systems of any other person or organization. However, employees must be aware that any information
stored on or communicated through the BCN may be susceptible to "hacking" by a third party.

24) Accessing web sites, newsgroups, or chat areas that contain material that is obscene, pornographic, illegal and/or that promotes illegal acts (whether visual or written). Likewise, using the BCN to share or post obscene, pornographic and/or illegal material or material that promotes illegal acts (whether visual or written), or contains dangerous recipes, formulas, or instructions.

25) Accessing newsgroups, chat rooms, list servers, or other services where users may communicate with people outside of SWBOCES (including e-mail) except for work related purposes, except as otherwise provided in Policy 6413. While some incidental personal use of such services may be permitted, such incidental use will not be deemed a waiver of SWBOCES' right to prohibit all such use, either on an individually applicable or on a generally applicable basis.

26) Engaging in "spamming" (sending an electronic communication for non-workrelated purposes to any SWBOCES employee).

27) Posting anonymous messages or forging e-mail or other messages.

28) Intentionally disrupting information network traffic or crashing the BCN and connected systems; SWBOCES users must not degrade or disrupt equipment or
system performance. SWBOCES users must not download or save excessively large files without the express approval of the network administrator.

29) Taking data, equipment, software, or supplies (paper, toner cartridges, disks, etc.) for their own personal use. Such taking will be treated as theft. Use of SWBOCES printers and paper for personal use is not permitted.

30) Refusing or failing to return SWBOCES-issued electronic devices, such as smart phones and laptops, when directed to do so by SWBOCES or upon separation from service.

31) Deleting, copying, and/or altering any data, information, or software/applications from SWBOCES-issued electronic devices, such as smart phones and laptops, prior to returning such devices to the SWBOCES.

32) Sharing confidential information on students and/or employees without authorization. Administrative or staff access is limited to portions of the BCN

necessary for the staff member to perform his/her job responsibilities. Access to unauthorized areas of the BCN is prohibited due to the confidential nature of the
information contained therein.

33) Data Management

a) Storing confidential or personally identifiable data related to students and/or employees on any unauthorized personal storage device or application,
including a personal cloud or social media sites.

b) Sending, forwarding, sharing, or storing email and/or attachments containing personally identifiable data of students and/or employees within SWBOCES
or the data housed by the Lower Hudson Regional Information Center (LHRIC) for component school districts without authorization or the proper
encryption protocols.

c) Providing data to any person or organization, under any circumstance, without the permission of an authorized representative of SWBOCES or the LHRIC.

34)Using the BCN for purposes other than SWBOCES-related work or activities, except as otherwise provided in Policy 6413.

35) Using any personal devices, including but not limited to, laptops, tablets, cellular devices, etc.) for work-related purposes under any circumstance. All employees will be provided with access to an authorized SWBOCES technology device based on their role. Personal cell phones or personal smartphones that are approved for use by the Assistant Superintendent for Business and Administration, under Policy 4341, are permitted for work related purposes.

Use of other Networks or Resources
Any user of the BCN that accesses another network or other computer resources shall be subject to that network's acceptable use policy as well as the SWBOCES policy and regulation. Where a conflict exists between policies, SWBOCES policy and regulation will govern.

Passwords
Password Requirements – All users will be required to change their password periodically, every 90 days. At a minimum, all passwords will adhere to complexity requirements of eight (8)characters, including at least one number and one capital letter in the password. The password complexity requirements are subject to change without notice to meet industry best practices.

Sanctions

Additional reports of inappropriate behavior, violations, or complaints will be referred to the staff member's supervisor for appropriate action. Violations may result in a loss of access to the BCN and/or disciplinary action. When applicable, law enforcement agencies may be involved.

Notification
All staff have access to SWBOCES policies on staff and student acceptable use and the regulations established in connection with those policies. Each staff member must sign off acknowledging that they have read, understand, and agree to Policy 6413 and this regulation before establishing an account or continuing their use of the BCN.

NOTE: Refer also to Policy #6413—Staff Acceptable Use Policy