

Personnel

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES

The BOCES computer system (BCS hereafter) is provided for staff to enhance the educational programs of the BOCES, to further BOCES goals and objectives; and to conduct research and communicate with others.

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance shall apply to use of the BCS. The standards of acceptable use as well as prohibited conduct by staff accessing the BCS, as outlined in BOCES policy and regulation, are not intended to be all-inclusive. The staff member who commits an act of misconduct which is not specifically addressed in BOCES policy and/or regulation may also be subject to disciplinary action, including loss of access to the BCS as well as the imposition of discipline under the law and/or the applicable collective bargaining agreement. Legal action may also be initiated against a staff member who willfully, maliciously or unlawfully damages or destroys property of the BOCES or its networks.

Staff are encouraged to utilize electronic communications in their roles as employees of the BOCES. Staff are also encouraged to utilize electronic means to exchange communications with parents/guardians or homebound students, subject to appropriate consideration for student privacy. Such usage shall be limited to school related issues or activities. Communications over the BCS are often public in nature; therefore, general rules and standards for professional behavior and communications will apply.

The BOCES's policies and accompanying regulations on staff and student use of computerized information resources establish guidelines for staff to follow in instruction and in working with students on acceptable student use of the BCS, including access to external computer networks.

Privacy Rights

Staff data files, email and electronic storage areas shall remain BOCES property, subject to BOCES control and inspection. The computer coordinator may access all such files and communications without prior notice. Staff should **NOT** expect that information stored on the BCS will be private as there is no expectation of privacy in such information.

Prohibitions

It is not the intention of this regulation to define all inappropriate usage. However, in addition to the general requirements of acceptable staff behavior, activities which shall be prohibited by staff members using the BCS include, but are not limited to, the following:

- 1) Using the BCS which in any way results in unauthorized charges or expense to the BOCES.

(Continued)

Personnel

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES (Cont'd.)

- 2) Damaging, disabling or otherwise interfering with the operation of computers, computer systems, software or related equipment through physical action or by electronic means.
- 3) With the exception of educational software installed and/or modified by a Network Administrator for instructional purposes, users may not add any software or applications to the BCS, or add to or modify any existing software or applications, without the express permission of the network administrator. Any software that is installed must be properly licensed from the copyright owner thereof, and any modifications must comply with the terms of the applicable license(s) and meet all NYSED Data privacy compliance requirements.
- 4) Changing, copying, renaming, deleting, reading or otherwise accessing files or software not created by the staff member without express permission from the computer coordinator.
- 5) Violating copyright law, including the illegal file sharing of music, videos and software.
- 6) Employing the BCS for commercial purposes, product advertisement or political lobbying.
- 7) Disclosing an individual password to others or using others' passwords.
- 8) Sharing confidential information on students and employees. Administrative or staff access is limited to portions of the BCS necessary for the staff member to perform his/her job responsibilities. Access to unauthorized areas of the BCS is prohibited due to the confidential nature of the information contained therein.
- 9) Sending or displaying offensive messages or pictures.
- 10) Harassing, insulting, bullying, threatening or attacking others.
- 11) Engaging in practices that threaten the BCS (e.g., loading files that may introduce a virus).
- 12) Violating regulations prescribed by the network provider.
- 13) Except as otherwise provided in the Policy 6410, use of the BCS for other than school related work or activities.
- 14) Assisting a student, staff or any other person to violate BOCES policy and/or regulation, or failing to report knowledge of any violations of the BOCES's policy and regulation on student and/or staff use of computerized information resources.

- 15) Use which violates any other aspect of Policy 6410 and/or its regulations, as well as local, state or federal laws or regulations.
- 16) Software Selection: all software requests (local installs, web based, or mobile apps) must be submitted to a supervisor for review and approval in conjunction with the SWBOCES Technology Department. 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.
- 17) Except as otherwise provided for in the BOCES Policy 6410, use of audio/video streaming services (YouTube, Pandora, Netflix, Amazon Prime, etc..) is not permitted unless it is part of a work related task and/or assignment, (ie. Presentations, classroom teaching, etc...).
- 18) Using vulgar, derogatory, or obscene language.
- 19) Posting anonymous messages or forging e-mail or other messages.
- 20) 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 BCS may be susceptible to "hacking" by a third party.
- 21) Accessing Web Sites, newsgroups, or chat areas that contain material that is obscene or that promotes illegal acts. Likewise, using the BCS to access or process pornographic material (whether visual or written), or material which contains dangerous recipes, formulas or instructions, is prohibited.
- 22) Except as otherwise, provided in the BOCES Policy 6410, accessing newsgroups, chat rooms, list servers, or other services where they may communicate with people outside of the BOCES (specifically including e-mail) except for work related purposes. While some incidental personal use of such facilities may be permitted, such incidental use will not be deemed a waiver of the BOCES' right to prohibit all such use, either on an individually-applicable or on a generally-applicable basis.
- 23) Engaging in "spamming" [sending an electronic communication for non-work related purposes to any BOCES employee].
- 24) Maliciously accessing, altering, deleting, damaging or destroying any computer system, computer network, computer program, or data. Such BOCES users will be subject to criminal prosecution as well as to disciplinary action by the BOCES. 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, furniture or any BOCES property.
- 25) Intentionally disrupting information network traffic or crashing the BCS and connected systems; BOCES users must not degrade or disrupt equipment or system performance.

BOCES users must not download or save excessively large files without the express approval of the network administrator.

- 26) BCS users must 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. The BOCES library professionals can assist employees with fair use issues.
- 27) Copying any copyrighted or licensed software from the Internet, from the BCS 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 BOCES owned device.
- 28) 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 BOCES printers and paper for this purpose is not permitted
- 29) Data Management: Employees will not
 - a) store confidential or personally identifiable data on any personal storage, either in the cloud, including social media sites, or on local devices that are not encrypted or password protected.
 - b) email attachments containing private data (Personally Identifiable Information) of students and employees within BOCES or the data housed by the LHRIC for component BOCESs.
 - c) provide data to any person or organization, under any circumstance, for any reason without the permission of an authorized representative of the BOCES/LHRIC or BOCES.

Any user of the BCS that accesses another network or other computer resources shall be subject to that network's acceptable use policy as well as the BOCES policy and regulation.

Sanctions

The computer coordinator will report inappropriate behavior to the staff member's supervisor who will take appropriate disciplinary action. Any other reports of inappropriate behavior, violations or complaints will be routed to the staff member's supervisor for appropriate action. Violations may result in a loss of access to the BCS and/or disciplinary action. When applicable, law enforcement agencies may be involved.

Notification

All staff will be given a copy of the BOCES's policies on staff and student use of computerized information resources and the regulations established in connection with those policies. Each staff member will sign an Acceptable Use Agreement (Form #6410F) before establishing an account or continuing their use of the BCS.

Adopted
09/28/2016

