Eastern Suffolk BOCES
Educational Services That Transform Lives

First Supervisory District of Suffolk County
201 Sunrise Highway
Patchogue, New York 11772

Regulation

Student Use of Electronic Communications and Telecommunications Equipment

Eastern Suffolk BOCES recognizes that effective use of technology is important to our students and will be essential to them as adults. Consequently, ESBOCES provides access to various electronic information resources through the ESBOCES Communication Systems (hereinafter referred to as the "BCS"), consisting of software, hardware, computer networks, and electronic communications systems. This may include access to electronic mail, "on-line services," "WiFi," and the "Internet." Student access to the BCS is a privilege, not a right.

The standards of acceptable use as well as prohibited conduct by students accessing the BCS as outlined in ESBOCES policy and regulation are not intended to be all-inclusive. Students are held to the same standards of good behavior whether they are using ESBOCES computer networks or any other electronic media or communications, including a student's own personal technology or electronic device, while on ESBOCES premises or at ESBOCES events. In addition to the specific standards of student conduct delineated in this regulation, the general requirements of acceptable student behavior expected under the ESBOCES Code of Conduct and the Dignity for All Students Act also apply to student access to the BCS. Communications on the network are often public in nature. General ESBOCES rules for behavior and communications apply.

Legal and ethical implications of software use will be taught to students of all levels where there is such software use. In addition, the Building Principal or his/her designee and/or classroom teacher will be responsible for informing students of rules and regulations governing student access to the BCS.

The following guidelines govern the management and general student use of the BCS, which includes all the various electronic information resources provided to ESBOCES students. These information resources include computer hardware, software, networks, e-mail, on-line services, Internet, videoconferencing, and other electronic communication systems such as telephones, fax machines, photocopiers, personal data systems, hardware and software storage devices, and the like. Board Policy 5112 and Administrative Regulation 5112R.1 exist to govern employee use of the BCS. Only authorized employees (under the supervision of an ESBOCES administrator) may access and/or monitor files and communications to ensure integrity and to verify that students are complying with Board policies and administrative regulations. Students should expect that information stored on the BCS will not be private and may be subject to discovery in a disciplinary and/or legal proceeding.

Use of ESBOCES Communication Systems (BCS)

BCS use is governed by Board policies and administrative regulations as well as Federal, State, and local laws. All students have a responsibility to utilize the BCS in an appropriate, lawful, and ethical manner. Students using the BCS are expected to conform to the standards of behavior as outlined in the ESBOCES Code of Conduct. Inappropriate use of the BCS may result in disciplinary action, including suspension or cancellation of access. Prior to suspension or revocation of access to the BCS, students will be afforded an informal opportunity to discuss the factual situation underlying the reasons for such suspension or revocation with the appropriate administrator/supervisor. Each student who is granted access will be responsible for that usage.

The BCS is provided for students in support of their educational program and to conduct research and communicate with others. Likewise, students are expected to observe the same standards of behavior when using their own personal technology or electronic devices on ESBOCES premises or at ESBOCES events. Individual users of the BCS are responsible for their behavior and communications over the ESBOCES computer network. It is presumed that users will comply with ESBOCES standards and will honor the agreements they have signed.

Student data files and other electronic storage areas shall be considered to be ESBOCES property and subject to ESBOCES control and inspection. Appropriate administrative staff may access all such files and communications without prior notice to ensure system integrity and that users are complying with the requirements of ESBOCES policy and regulations regarding student access to the BCS. Students should **NOT** expect that information stored on the BCS will be private.

While at ESBOCES, teachers will guide students toward appropriate materials. Outside of ESBOCES, parents/guardians bear responsibility for such guidance as they do with information sources such as television, telephones, movies, radio, and other potentially offensive/ controversial media.

Use of the BCS which violates any aspect of ESBOCES policy; the Code of Conduct; and Federal, State, or local laws or regulations is strictly prohibited and may result in disciplinary action in compliance with applicable ESBOCES guidelines and/or Federal, State, and local law, including, but not limited to, suspension and/or revocation of access to the BCS.

The following standards of acceptable use and prohibited conduct in the use of the BCS are not intended to be all-inclusive. It is the intention of Board policy and administrative regulation, student orientation, and instructional programs to provide guidance that promotes appropriate use of the BCS. If a student is unsure whether a specific behavior not addressed by Board policy, administrative regulation, orientation or instruction constitutes an appropriate or inappropriate use of the BCS, it is the student's responsibility to seek guidance from an appropriate employee. The following are student guidelines for appropriate behavior when using the BCS.

User Guidelines

1. Students must obtain permission from an appropriate ESBOCES employee in order to connect to the BCS.

2. In instances where a student's name and/or password are necessary to access the BCS, students will identify themselves honestly.

3. Students shall not violate any Federal, State, or local laws or the Board policies or administrative regulations of ESBOCES while utilizing the BCS.

4. Students shall not use the BCS or their own equipment/devices to reveal, produce, or distribute information such as name, address, telephone number, photographic images, video images, or audio recordings (about themselves or others) without the permission of an appropriate ESBOCES employee.

5. Students shall not engage in bullying, threats, or personal attacks, including prejudicial, discriminatory, or insulting attacks or harassment. Students shall not knowingly or recklessly

share false or defamatory information about a person or an organization via any component of the BCS.

6. Students shall not display any kind of sexually explicit image or document on any component of the BCS. In addition, sexually explicit material shall not be accessed, archived, stored, distributed, edited or recorded using the BCS.

7. Students shall not utilize the BCS to obtain, view, download, send, print, display, or otherwise gain access to or transmit unacceptable or inappropriate material that is profane or obscene (pornography), unlawful, abusive, or that advocates or invokes illegal acts, violence, or discrimination. Students who inadvertently access such material must promptly notify an ESBOCES employee.

8. Students shall not utilize the BCS to download or distribute pirated or unauthorized software, data files, music, photographic images, video images, or audio recordings.

9. Students shall not use the BCS to download entertainment software, games, video, real-time audio, music, or real-time games without authorization from an appropriate ESBOCES employee.

10. Students shall not utilize software in ways that are inconsistent with their licenses or copyrights.

11. Students shall not violate copyright law, including the illegal file sharing of music, videos, and software.

12. Students shall not upload any software, data files, photographic images, video images, or audio recordings utilizing the BCS without the permission of an appropriate ESBOCES employee.

13. Students shall not utilize the BCS to facilitate cheating or plagiarize works accessed via the BCS or to misappropriate intellectual property.

14. Students shall not utilize the BCS to damage, disable, overload, or otherwise interfere with the operation of any communication system or network, or to circumvent any system intended to protect privacy or security, through physical action or electronic means.

15. Students shall not willfully utilize the BCS to propagate any virus, worm, Trojan horse, or trapdoor program code or other system-damaging software.

16. Students shall not actively seek security breaches within the BCS, as this may be construed as an illegal attempt to gain inappropriate access. Students who inadvertently discover a security breach of the BCS must promptly notify an ESBOCES employee.

17. Unless given permission by a supervisor/instructor, a student shall not exceed his/her authorized level of access, disclose an individual's password to others, or log in through another user's account. No student shall access files created by another user without that user's permission.

18. Students shall not change, copy, rename, delete, read, or otherwise access files or software of others without express permission from the creator of the file or his/her supervisor/instructor.

19. Students shall not post chain letters or engage in “spamming” (sending unsolicited e-mail to a large number of addresses) over the BCS.

20. Students shall not use the BCS for non-educational commercial purposes, such as offering or providing goods or services for personal gain. This does not preclude student involvement in authorized internships or other work-study experiences.

21. Students shall not purchase goods and/or services through the BCS.

22. Any student who accesses another network or other computer resource shall be subject to that network’s Acceptable Use Policy, as well as that of ESBOCES.

23. Students shall not access personal, interactive, social networking Web sites (such as Facebook) through the BCS unless under the direct supervision of an ESBOCES employee. This includes the use of a student's personal cellular telephone or electronic communication device through the BCS to access such social networking sites.

24. Students shall not create or use a Web site or blog through the BCS which may cause a substantial disruption in the educational environment or interfere with the rights of others.

If a student or a student's parent/guardian has an ESBOCES network account, a non-ESBOCES network account, or any other account or program which will enable direct or indirect access to an ESBOCES computer, any access to the BCS in violation of ESBOCES policy and/or regulation may result in student discipline. Indirect access to an ESBOCES computer shall mean using a non-ESBOCES computer in a manner which results in the user gaining access to an ESBOCES computer, including access to any and all information, records or other material contained or stored in an ESBOCES computer.

Management of System

ESBOCES has the right to monitor, log and inspect any and all aspects of the BCS and to report its findings as necessary in order to promote appropriate and efficient use and to ensure system integrity.

ESBOCES utilizes software and/or hardware solutions to limit and control use of the BCS.

ESBOCES utilizes and periodically updates filtering software to block inappropriate content; however, by its nature, this software is imperfect and does not guarantee that some questionable content may become available.

Any student who attempts to disable, defeat, or circumvent any ESBOCES security measures will be subject to disciplinary and/or legal action.

ESBOCES may periodically back up the E-mail system and networked data storage areas.

ESBOCES may issue user IDs to help maintain individual accountability for system resource usage. Each student may be assigned a password to be used in conjunction with his/her user ID. ESBOCES prohibits the sharing of passwords among students.

Internet usage will be monitored for all students using the BCS.

Administration of Board Policy and Administrative Regulation

Administrators (or their designees) will provide students and parents with copies of Board Policy 6216 - Student Use of Electronic Communications and Telecommunications Equipment, and this administrative regulation. In addition, all students will receive an explanation of the Board policy and administrative regulation. Students and parents will be provided the opportunity to ask questions so that they fully understand the Board policy and administrative regulation. ESBOCES will establish and implement a process whereby students and/or parents acknowledge in writing that they have read, understand, and agree to follow the Board policy and administrative regulation that have been adopted to promote acceptable use of the BCS. All such acknowledgements shall be kept on file in the building/program main office and renewed annually.

A review of a student's use of the BCS may be conducted if there is reasonable suspicion that the student has violated a law, Board policy, or administrative regulation.

Discipline

A student who commits an act of misconduct related to the BCS may be subject to disciplinary action in accordance with the ESBOCES Code of Conduct, including, but not limited to, the loss of access to any or all components of the BCS.

Legal action may be initiated against a student who willfully, maliciously, or unlawfully vandalizes, damages, or destroys property of ESBOCES.

Use of any ESBOCES resources for illegal activity may be grounds for disciplinary action as outlined in the ESBOCES Student Code of Conduct. When applicable, law enforcement agencies may be contacted, and ESBOCES will cooperate with any legitimate law enforcement process.

Notwithstanding the above, violations will be handled in accordance with due process procedures on a case-by-case basis.

Security

Security on any computer system is a high priority, especially when the system involves many users. Users of the BCS identifying a security problem on the BCS must notify the teacher in charge. A student is not to demonstrate the problem to other users. Attempts to log on to the BCS as an administrator may result in restriction or suspension of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the BCS. Further, any violations regarding the use and application of the BCS shall be reported by the student to the teacher in charge.

Authorization

Student use of the BCS is conditioned upon written agreement by all students and their parents/guardians that student use of the BCS will conform to the requirements of this policy and associated regulation to ensure acceptable use of the BCS. All such agreements shall be kept on file in the program/facility office.

References:

- Dignity for All Students Act
- Board Policy 6216 – Student Use of Electronic Communications and Telecommunications Equipment
- Administrative Regulation 2410R.1 – Code of Conduct

First Approved: 9/25/2001
Revised: 3/5/2007
Revised: 8/7/2007
Revised: 10/24/2011
Revised: 8/15/2013