

Southern Westchester BOCES Acceptable Use Policy for Technology and the Internet

BOCES Employees

The following Policy and Consent form must be read and signed by the employee before access will be provided to BOCES computer and Internet facilities.

Introduction

The BOCES furnishes computers and provides access to the Internet in order to support learning and enhance instruction. By providing access to the Internet, a vast information highway connecting thousands of computers all over the world, the Southern Westchester BOCES intends to promote educational excellence and to prepare students for an increasingly technological world. This use should facilitate resource sharing, research, innovation and communication.

However, the BOCES also recognizes that with this access comes the availability of material that is unrelated to scholarship, and which in many instances is inappropriate for places of learning.

For this reason, computers, network and Internet facilities are to be used primarily for BOCES-related purposes. Incidental personal use of BOCES computers must not interfere with the employee's job performance, must not violate any of the rules contained in this policy and must not damage BOCES' hardware, software, or computer communications systems.

Much of the responsibility for appropriate use of the Internet must rest on employees themselves. Therefore, the BOCES requires that employees act responsibly by reading and following the policies outlined below. Furthermore, employee use is contingent upon execution of a signed Consent and Waiver Agreement as annexed hereto.

Employees must understand that access to BOCES computer and Internet facilities is a revocable privilege, and not a right. Use of the system can and will be monitored by the BOCES, and there is no expectation of privacy in employee use.

Applicability and General Principles

These policies apply to all employees who gain access to the Internet via computer equipment and/or access lines located in the BOCES. This includes any remote access which employees may gain from off-site, but which involves the use of BOCES sites, servers, Intranet facilities, e-mail accounts or software.

The primary access to and use of the Internet must be for the purposes of work, teaching or scholarship consistent with the educational goals of the BOCES. Employees must make efficient, ethical and legal utilization of network resources. Employees must be aware that material created, stored on, or transmitted from or via the system is not guaranteed to be private. In addition to the fact that the Internet is inherently insecure, BOCES network administrators may review the system at any time to ensure that the system is working properly. For this reason, employees should expect that e-mails, materials placed on personal Web pages, and other work that is created on the network may be viewed by a third party.

External access will be provided to authorized users by the assignment of unique log-in identification codes (names and passwords) and, where appropriate, with limited hard disk space on BOCES hardware, for their own individual use. Authorized users will be personally

responsible for maintaining the integrity of the BOCES' access policy, and may not permit other persons to use their usernames, passwords, accounts or disk space, or disclose their usernames, passwords or account information to any third party.

Usernames and passwords will be furnished only to persons who have signed and returned a copy of this document, and such updates or modifications as may hereafter be promulgated. The users signature certifies that he/she has read this document, understands it, and agrees to be bound by its terms.

Users must respect the integrity and security of the BOCES' systems and network, and the access privileges, privacy and reasonable preferences of other users. The BOCES reserves the right to limit access time and disk space in order to optimize an equitable allocation of resources among users.

The BOCES makes no warranties of any kind, whether express or implied, for the service it is providing. It is not responsible for any damages, including loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions, whether caused by the BOCES' negligence, or by a users errors or omissions. Information obtained from the Internet is issued at the user's own risk, and the BOCES specifically disclaims any responsibility for the accuracy or quality of information obtained by employees via access provided by or through the BOCES.

The following policies are intentionally broad in scope and, therefore, may include references to resources, technology and uses not yet available.

Rules of Conduct and Compliance

Employees who violate this Acceptable Use policy may have their access privileges suspended or revoked by the network administrator. In addition, further disciplinary action may be taken as permitted by applicable law and the terms of any applicable collective bargaining agreement

Except as otherwise indicated below, all policies and prohibitions regarding users of the network also apply to users of individual BOCES computers.

With the exception of educational software installed and/or modified by a faculty member for instructional purposes, users may not add any software or applications to the BOCES' network or computers, 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).

2. The network may not be used for any commercial purposes.
3. The network may not be used for advertising, political campaigning, or political lobbying.
4. The network may not be used for any activity, or to transmit any material, that violates United States, New York State or local laws. This includes, but is not limited to, fraudulent acts, violations of copyright laws, and any threat or act of intimidation or harassment against another person.
5. The BOCES is a place of tolerance and good manners. Use of the network or any BOCES computer facilities for hate mail, defamatory statements, statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability is prohibited.

6. Network users may not use vulgar, derogatory, or obscene language.
7. Network users may not post anonymous messages or forge e-mail or other messages.
8. Network users may not log on to someone else's account, attempt to access another user's files, or permit 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 BOCES network may be susceptible to "hacking" by a third party.
9. Network users may not access' Web Sites, newsgroups, or chat areas that contain material that is obscene or that promotes illegal acts. Likewise, using the network to access or process pornographic material (whether visual or written), or material which contains dangerous recipes, formulas or instructions, is prohibited.
10. Users may not access newsgroups, chat rooms, list servers, or other services where they may communicate with people outside of the BOCES (specifically including e-mail) except for District business. 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.
11. Users may not engage in "spamming" (sending an electronic communication to more than 10 people at the same time) or participate in chain letters.
12. Users who maliciously access, alter, delete, damage or destroy any computer system, computer network, computer program, or data 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.
13. Users may not intentionally disrupt information network traffic or crash the network and connected systems; they must not degrade or disrupt equipment or system performance. They must not download or save excessively large files without the express approval of the network administrator.
14. 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.
15. Users may not copy any copyrighted or licensed software from the Internet, from the network or from another user without the express permission of the copyright holder: Software must be purchased or licensed before it can legally be used.
16. Users may not take 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 must be reasonable.

Violations and Consequences

Consequences of violations include but are not limited to:

- Suspension or revocation of information network access;
- Suspension or revocation of network privileges;

- Suspension or revocation of computer access;
- Disciplinary action, up to and including termination of services.

In addition, the BOCES will seek monetary compensation for damages in appropriate cases.

Repeated or severe violations will result in more serious penalties than one-time or minor infractions.

This Acceptable Use Policy is subject to change. The BOCES reserves the right to restrict or terminate information network access at any time for any reason. The BOCES further reserves the right to monitor network activity as it sees fit in order to maintain the integrity of the network and to monitor acceptable use. School and District-wide administrators will make final determination as to what constitutes unacceptable use.

Disciplinary penalties involving adverse employment action will be determined in accordance with applicable state law and the terms of applicable collective bargaining agreements. However, by signing the Consent attached to this Acceptable Use Policy, employees agree that suspension or revocation of access privileges will be determined by the network administrator, acting in consultation with School and District-wide administrators.

The Consent and Waiver Agreement, which appears on the following page, must be signed and returned by the employee as a condition of access to BOCES computer and Internet facilities.