

Board

Employee/Board Member Use of ESBOCES Communication Systems

Acceptable Use and Internet Safety

System Definition

Eastern Suffolk BOCES provides its employees and Board members (hereinafter collectively referred to as “users”) with access to electronic information resources, including, but not limited to computer hardware, software, networks, electronic communication systems, telephones, fax machines, photocopiers, and smart phones through the ESBOCES Communication Systems (BCS). ESBOCES, through appropriate levels of administration and staff, shall monitor the use of the Internet/computer networks authorized by this policy. Any inappropriate use of hardware, software, or access to information on the Internet or computer network may result in the cancellation of user accounts. This may include access to electronic mail (e-mail), social networking sites, texting, online services, Wi-Fi, and the Intranet/Internet. It may also include the opportunity for users to have independent access to the BCS from remote locations. All use of the BCS, including independent use off ESBOCES premises, shall be subject to this Board policy and Administrative Regulation 5112R.1 – *Employee/Board Member Use of ESBOCES Communication Systems*.

Purpose

The goal of ESBOCES in providing Internet and computer network services to employees is to promote educational excellence by facilitating resource sharing innovations and communications and engage in work-related professional communication to further the mission of ESBOCES. It is anticipated that access to various electronic information resources will expedite and enhance the performance of work-related tasks and assignments. To that end, ESBOCES shall provide orientation for this Board policy and the related administrative regulation.

Acceptable/Unacceptable Use

The use of a network account must be in support of education and research, consistent with the educational objectives of ESBOCES. Transmission of any material in violation of any United States or State regulation or ordinance is prohibited. This includes, but is not limited to copyrighted material, threatening or obscene material, or material protected by trade secret. Use for commercial activity is prohibited. Use for product advertisement or political lobbying is also prohibited. ESBOCES shall have no responsibility for any misuse of the accounts granted under this policy, and such misuse may result in discipline, any other appropriate penalty (e.g., suspension or revocation of user’s access to network), and/or may be reported to the authorities.

This policy does not attempt to articulate all required and/or acceptable uses of the BCS, nor is it the intention of this policy to define all inappropriate usage. Administrative regulations will further describe general guidelines of appropriate conduct and use as well as proscribed behavior, including:

1. Interacting with other individuals on social networking platforms, and

2. cyberbullying awareness and response.

The use of the Internet/Computer Network is a responsibility, not a right, and inappropriate use may result in cancellation of such account(s). Note that electronic mail (e-mail) and data files are not guaranteed to be private. People who operate the systems do not have access to all e-mail and data. ESBOCES has access to all e-mail and data. Message(s) or other electronic data relating to or in support of illegal activities may be reported to the authorities and the Chief Operating Officer, District Superintendent, or designee.

Student Communication

Do not “friend,” “follow,” or otherwise interact with students from your personal social media accounts. Be aware that even with the most stringent privacy settings, photo tagging and other tools may make personal information regarding students and their families publicly available. Staff must avoid posting student information, pictures, and work-product exemplars on personal social media sites, blogs, or any other social media that is not specifically authorized by ESBOCES. Employees who choose to communicate with students and families through text messages should, whenever possible, do so using an ESBOCES-provided device or ESBOCES-supported technology. Employees who use their own personal devices to communicate with students and families must do so in a professional manner and limited to the scope of the staff member’s ESBOCES responsibility.

Use of the BCS shall cease and the equipment returned to ESBOCES or the user’s access revoked under the following circumstances, including, but not limited to:

1. a user separates from service as an employee or Board Member of ESBOCES;
2. status as a person authorized to access the BCS or use ESBOCES equipment terminates;
or
3. a user is assigned a new position and/or responsibility pursuant to which use of the BCS, or a portion thereof, has not been authorized.

Anyone who is aware of any misuse or abuse of any software or electronic communication system owned or leased by ESBOCES shall notify his/her immediate supervisor or building principal.

An administrator who is aware of any misuse or abuse shall notify the District Superintendent, Chief Operating Officer, or designee, and appropriate disciplinary action may occur based on the circumstances and in accordance with all applicable laws, bargaining agreements, Board policies, and administrative regulations.

Limitation of Liability

ESBOCES will make reasonable efforts to assist users who are experiencing work-related technical problems. However, ESBOCES makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the BCS will be error-free or without defect. ESBOCES will not be responsible for damages users may incur, including, but not limited to, loss of data or interruptions of service. ESBOCES is not responsible for the accuracy or quality of the information obtained through or stored on the BCS. ESBOCES will not

be responsible for obligations, financial or otherwise, incurred as a result of the unauthorized use of the BCS.

Privacy

No Expectation of Privacy - Users are provided access to components of the BCS, including, but not limited to, computers, computer accounts, data files, smart phones, and electronic storage areas to assist them in performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send or receive on the computer system. By accessing/using the BCS, the user has consented to ESBOCES exercising its authority and the rights set forth in this policy, including the right to monitor any information or communication stored or transmitted over the BCS.

Waiver of Privacy Rights - Users expressly waive any right of privacy in anything they create, store, send, or receive through the BCS, including on the computer. Users consent to allow ESBOCES employees to access and review all materials users create, store, send, or receive through the BCS, including the computer and through computer networks and the Internet. Users understand that ESBOCES may use human or automated means to monitor use of the BCS resources.

References:

- Board Policy 5122 – Employee-Student Relations (Fraternization)
- Board Policy 5220 - Employee Personnel Records and Release of Personnel Information
- Board Policy 6216 – Student Use of Electronic Communications and Telecommunications Equipment
- Administrative Regulation 5112R.1 – Employee/Board Member Use of ESBOCES Communication Systems

First Adopted: 9/25/2001
Readopted: 7/1/2003
Readopted: 12/21/2006
Readopted: 7/11/2007
Readopted: 12/15/2010
Readopted: 1/23/2013
Readopted: 8/29/2018
Readopted: 12/10/2025